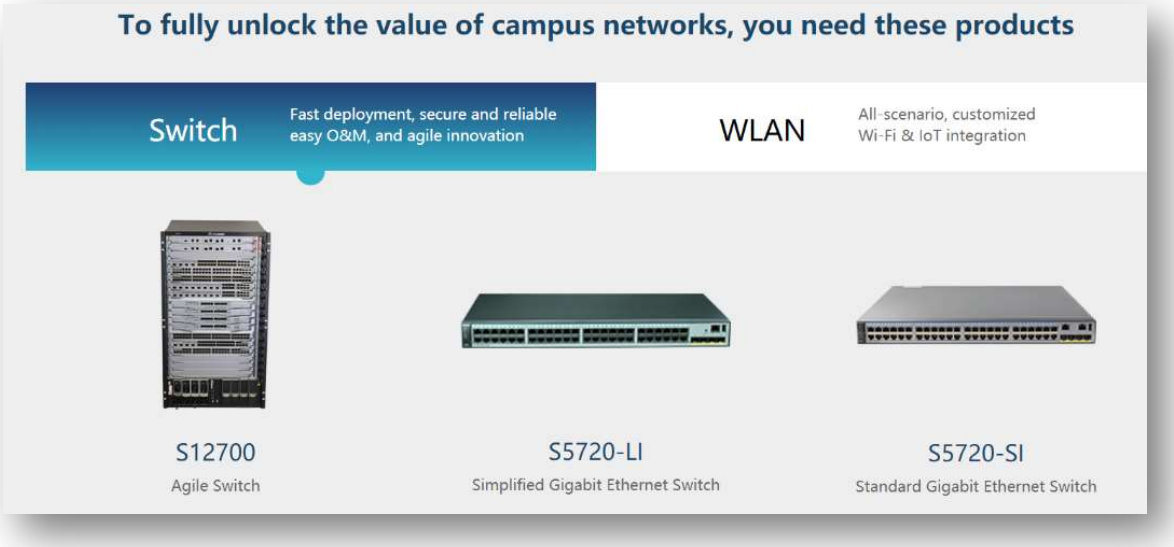
***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

Harris Corporation expressly reserves the right to supplement or modify these Disclosures as appropriate upon receipt of further information and discovery. The Huawei '678 Patent Accused Products (as that term is defined and the corresponding devices are identified in Harris's P.R. 3-1 and P.R. 3-2 disclosures cover pleading) infringe at least the following claims. References to instrumentalities in this chart are exemplary only and should not be construed as limiting the scope of any claim of the '678 patent. The Huawei '678 Patent Accused Products satisfy each claim element below literally. The Huawei '678 Patent Accused Products also satisfy claim elements under the Doctrine of Equivalents, including without limitation where specifically identified below, because they include and perform substantially similar functionality.

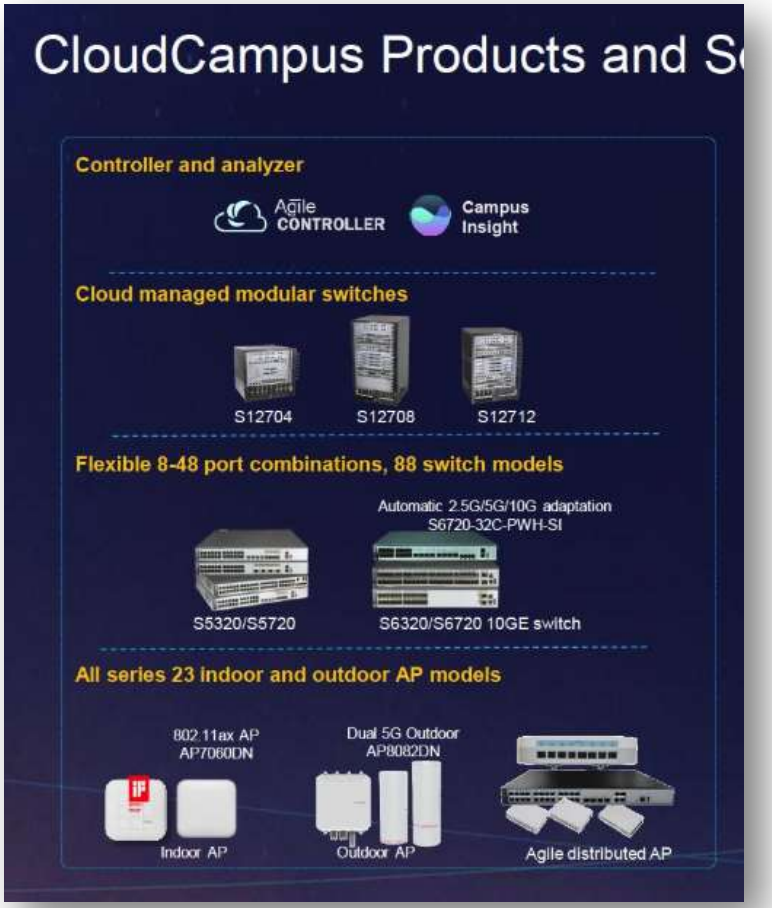
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
A wireless local or metropolitan area network comprising:	The Huawei '678 Patent Accused Products infringe this claim. Huawei makes, uses, sells, offers to sell and/or imports equipment used in wireless local or metropolitan area networks, including its WLAN products and consumer devices, and on information and belief, makes, uses, sells, offers to sell and/or imports wireless local or metropolitan area networks in the United States. Without the benefit of discovery, Harris identifies exemplary networks, including, without limitation, networks deployed at Huawei's 13 U.S. facilities; networks deployed in CloudCampus solutions such as those deployed for Cloud4Wi, in San Francisco, CA; other enterprise networks deployed for Weichai Power in Chicago, Ill., and Crowley Independent School District in Crowley, Tx. On information and belief, Huawei's United States Offices utilize the Huawei WLAN products to form a wireless local or metropolitan area network (Wireless LAN/MAN). These offices include Huawei Technologies USA, Inc. HQ's offices in Plano, Texas; Broomfield, CO; Houston, TX, Reston, VA; Philadelphia, PA; Irvine, CA; Cupertino, CA; Huawei Device USA, Inc. HQ's offices in Plano, Tx; Bellevue, WA; Mountain View, CA; Alpharetta, GA; Bridgewater, NJ; Santa Clara, CA; and San Diego, CA, as well as Futurewei Technologies, Inc.'s offices in Santa Clara, CA; Plano, TX, Bridgewater, NJ; Rolling Meadows, IL; Greensboro, NC; Louisville, CO; San Diego, CA; and Bellevue, WA. https://www.huawei.com/us/contact-us#office

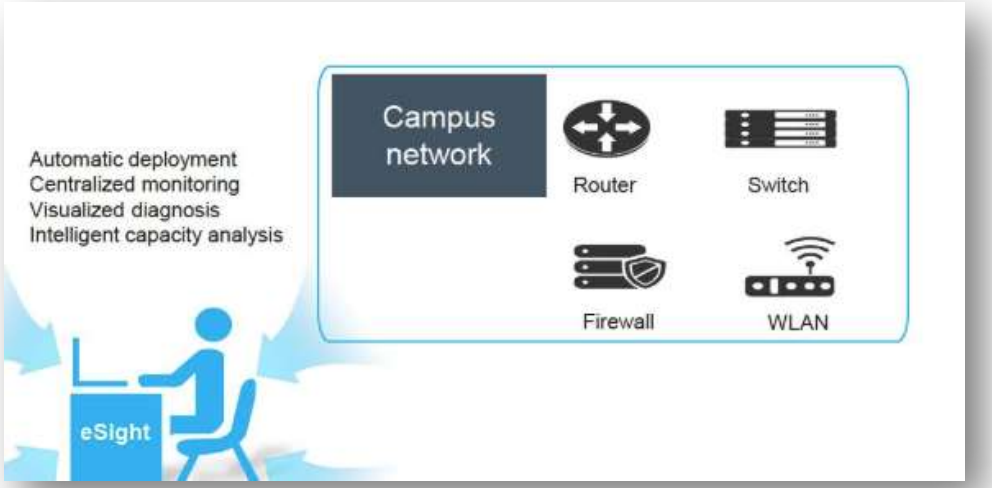
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Further, in 2017, Huawei partnered with Cloud4Wi in San Francisco California to install its CloudCampus solution. *See* https://cloud4wi.com/cloud4wi-and-huawei/ Huawei CloudCampus solutions utilize various switches and access points, for example: 

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 http://e.huawei.com/topic/cloudcampus-en/index.html

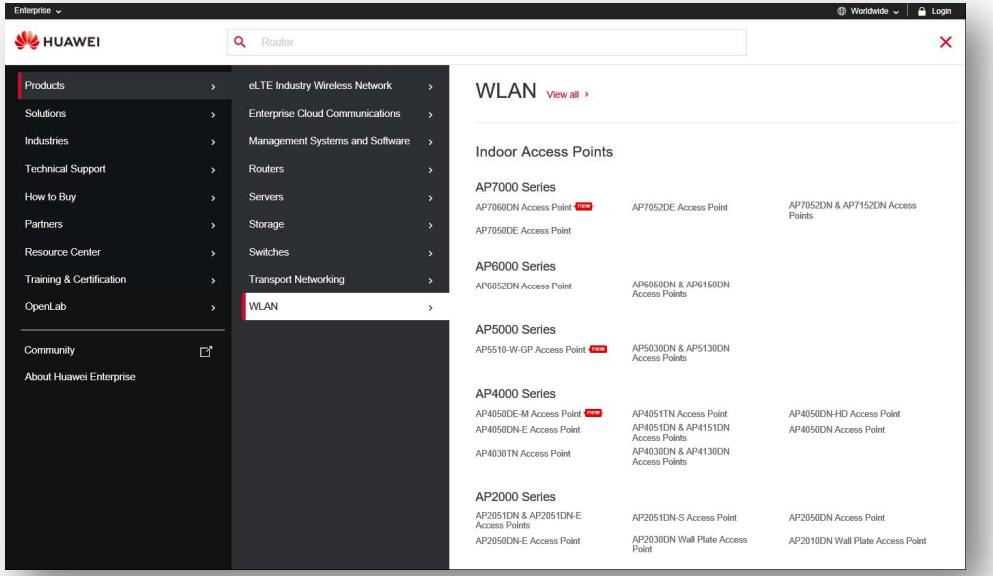
***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 https://e.huawei.com/en/material/onLineView?MaterialID=0b6395888b2a4bd49613a9bc28f3e95c at 15.

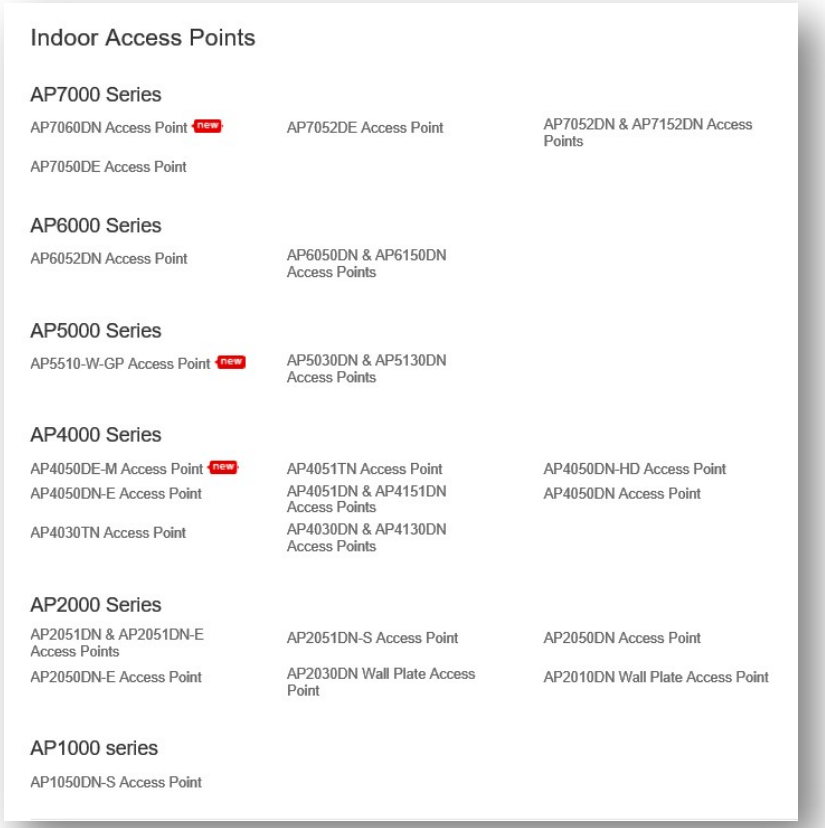
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Further, Campus networks are an exemplary network that may work with Huawei eSight:  eSight Overview Presentation at 6. On information and belief, all Huawei WLAN products incorporate the Wireless Intrusion Detection System (WIDS) as described, for example in the WIDS and WIPS Technology White Paper: "The Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions monitor and prevent the preceding attacks on WLANs. This document describes WIDS and WIPS technologies used by Huawei WLAN products." Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 1.

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei website currently lists the following WLAN products:

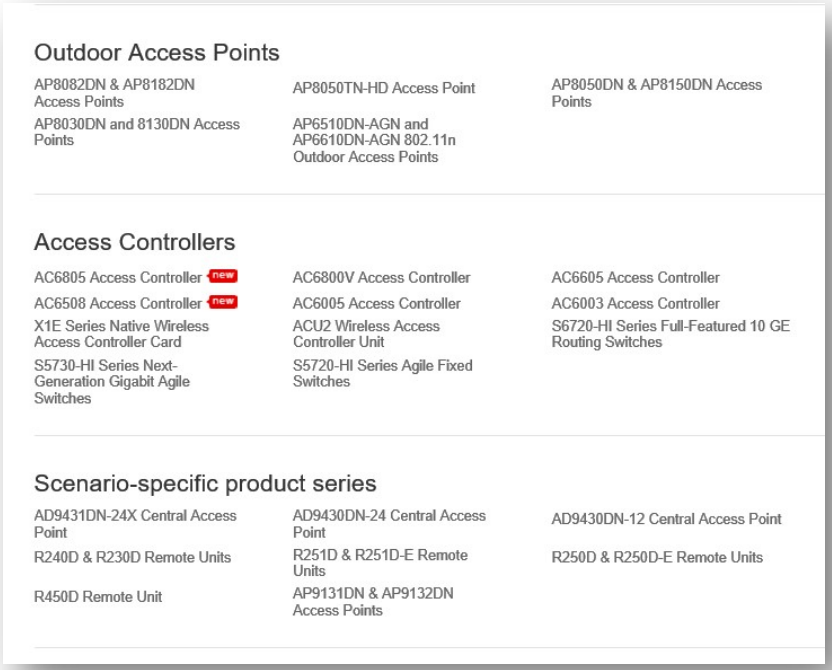


***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION



https://e.huawei.com/us/products/enterprise-networking/wlan (as of March 13, 2019).

See also, e.g., Huawei Access Point Datasheets ("*Rogue device monitoring Huawei APs support WIDS/WIPS, and can monitor, identify, defend, counter, and perform refined management on the rogue devices, to provide security guarantees for air interface environment and wireless data transmission."*) On information and belief, all APs support WIDS, *see also, e.g.,* AP2030DN at 2; AP4050DN-E at 3; AP4051DN & AP4151DN at 3; AP8050DN & AP8150DN at 3; AP6052DN at 4; AP6050DN&AP6150DN at 4. *See also* AP3050DE Product Description, *available at* https://support.huawei.com/enterprise/en/wlan/ap3050de-pid-

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	23482930?offeringId=21946538, at 13 ("Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist"); Huawei AP7060DN Access Point Data Sheet, *available at* https://e.huawei.com/en/related-page/products/enterprise-network/wlan/indoor-access-points/ap7060dn/wlan-ap7060dn, at 3 ("Huawei APs support WIDS/WIPS, . . ."). *See also,* Huawei Enterprise AP Series 802.11ac Brochure: For enterprise networks of different types and scales, Huawei offers the following AP models: 802.11ac indoor 7X30 series and 5X30 series APs, outdoor 802.11ac 8X30 series APs, and 802.11ac AP9130DN vehicle-mounted APs specially designed for rail transit communications.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION

Table 5-2 Features of Huawei 802.11ac APs

Huawei 802.11ac AP	AP5030DN/ AP5130DN	AP7030DE	AP8030DN/ AP8130DN	AP9130DN
Target market	Mid-range market: small- to medium-sized enterprises	High-end market: medium- to large-sized enterprises	Large campus outdoor coverage or backhaul	Rail transit
Working mode	Fit/Fat AP	Fit AP	Fit/Fat AP	Fat AP
Dying gasp	-	√	√	√
Wireless positioning/ Real-Time Location System (RTLS)	√	√	√	-
Spectrum analysis	√	√	√	-
Seamless roaming	√	√	√	√
IPv6	√	√	√	√
Wireless Intrusion Prevention System (WIPS)/Wireless Intrusion Detection System (WIDS)	√	√	√	√

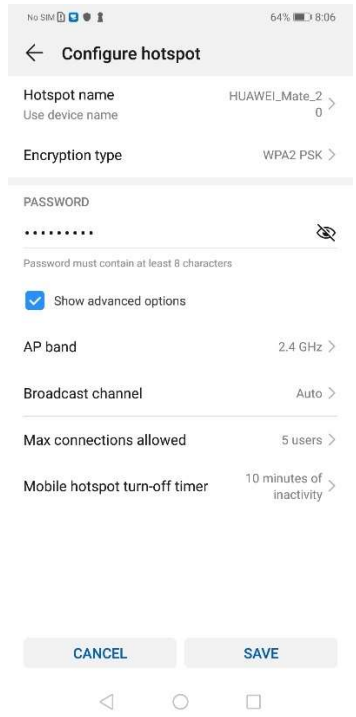
Huawei Routers deployed in a WLAN have various other security mechanisms, including:

"3.2.4 Security

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	… NAC Network Admission Control (NAC) is an end-to-end access security framework and includes… MAC address authentication" Huawei AR120&AR150&AR160&AR200&AR500&AR510&AR1 200&AR2200&AR3200&AR3600 Series Enterprise Routers Product Description, Issue 05 (2016-06-15) at 43. Routers may further operate as an Access Controller and provides MAC address authentication for WLAN: "3.2.6 WLAN A wireless local area network (WLAN) connects two or more computers or devices and enables the devices to communicate by using the wireless telecommunication technology. WLAN uses the wireless technology to implement fast Ethernet access. The primary advantage of WLAN is that terminals, such as computers, can access a network through a wireless medium rather than a physical cable. This facilitates network construction and allows users to move around without interrupting communication. WLAN is more flexible than traditional wired access. WLAN is widely used in public areas such as on campuses, business centers, and airports. The WLAN uses cables at the backbone layer, and users access the WLAN through one or more access points (APs) using radio waves. The transmission distance of an AP is tens of meters. IEEE 802.11 is widely used by WLANs. The device can function as an access controller (AC) or a Fat access point (FAT AP). The device as the AC or Fat AP supports 802.11a, 802.11b, 802.11g, 802.11an, and 802.11n.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	NOTE Only AR121W, AR129W, AR121GW-L, AR129GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161FGW-L, AR169W, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR510 series, AR503GW-LM7, AR503GW-LcM7, AR1220W, AR1220EVW and AR1220VW support WLAN-FAT AP. The device supports the following WLAN features: – WLAN user management – Dot1X access authentication – MAC address authentication – Pre-share-key (PSK) authentication – EAPOL-Key negotiation – User access control – AAA for WLAN users Huawei AR120&AR150&AR160&AR200&AR500&AR510&AR1 200&AR2200&AR3200&AR3600 Series Enterprise Routers Product Description, Issue 05 (2016-06-15) at 47. *See also, e.g.,* Huawei Remote Unit Datasheets: R450D at 6 ("*Security features - WIDS including rogue AP and STA detection, attack detection, STA/AP blacklist and whitelist… -Intrusion prevention"*); R251D & R251D-E ("*Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist*")

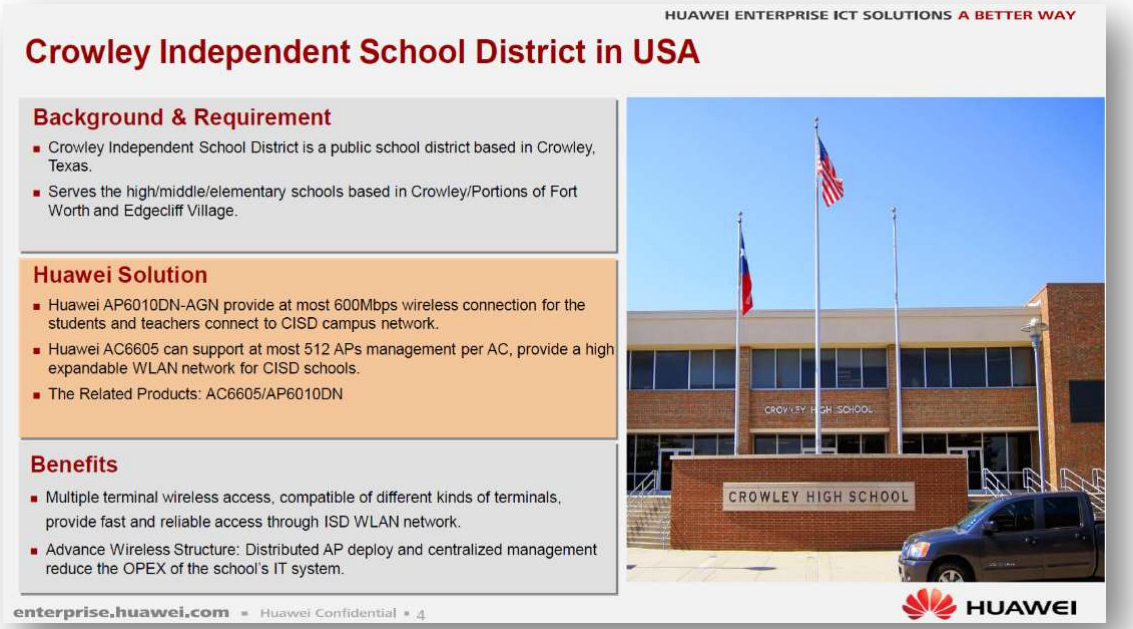
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	See also, e.g., Huawei Access Points (FATAP), V200R007C20, MIB Reference, Issue 05 (2019-03-15), *available at* https://support.huawei.com/enterprise/en/doc/EDOC1000154350, at Table 1 (listing products), 145-146, 1447-1515 and 2638-2712 (WIDS), 2790-2848 ("Station" / "STA" tables). Huawei consumer devices, including laptops, phones and tablets, are also designed to communicate with wireless networks via the IEEE 802.11 protocols. For example, specifications for Huawei smartphones such as the Huawei Mate SE indicate that they support "802.11b/g/n, 2.4 GHz" connectivity and the "Android N+EMUI 5.1" operating system. https://consumer.huawei.com/us/phones/mate-se/specs/. Specifications for Huawei's Mate 10 Pro smartphones indicate that they support "Wi-Fi 2.4G/5G, 802.11a/b/g/n/ac with Wi-Fi Direct support" connectivity and the "Android 8.0" and "EMUI 8.0" operating system. https://consumer.huawei.com/us/phones/mate10-pro/specs/. Specifications for Huawei laptops and tablets such as the Matebook 13 indicate that they support "IEEE 802.11a/b/g/n/ac" connectivity. https://consumer.huawei.com/en/laptops/matebook-13/specs/. Observation and testing of a Huawei Matebook 13 SE laptop and a Huawei Mate 20 phone both purchased in the United States demonstrate that the devices connect to and communicate with Wi-Fi networks, including at 2.4 GHz and 5 GHz speeds. Huawei consumer devices, including laptops, phones and tablets, also participate in the WIDS system as client stations (also referred to in WIDS and documentation as "STAs" or "ad hoc" devices). *See, e.g.*, Huawei Technologies Co., Ltd., *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 7 ("When receiving a Probe Request, an Association Request, or a Reassociation Request frame, the AP determines whether the sender is an ad hoc device or STA based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame") *see also id.* at 11 ("Rogue STAs: After detecting a rogue STA, a monitor AP uses the BSSID and MAC address of the rogue STA to send a fake unicast Deauthentication frame to contain it. A STA whitelist can also be configured to prevent STAs in the STA whitelist from associating with rogue APs"). *See also* Huawei Access Points (FATAP), V200R007C20, MIB Reference, Issue 05 (2019-03-15), at 145-146 (MAC authentication table), 1447-1515 and 2638-2712 (WIDS), 2790-2848 ("Station" / "STA" tables). Accordingly, and as further detailed herein, these devices implement aspects of the WIDS system within the "wireless local or metropolitan area network" of the claim (also referred to as a Wireless LAN/MAN in the patent specification).

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	On information and belief Huawei consumer devices, including laptops, phones and tablets also can participate in the WIDS system as access points ("APs"), including when configured as a mobile hotspot. For example, a Huawei Matebook 13 SE laptop and a Huawei Mate 20 phone both purchased in the United States allow configuration as, can operate as, and can connect to the other as, a mobile WiFi Hotspot:    Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also implement intrusion detection

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	according to the claim. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security."). Examination of the Android Manifest for a Huawei Mate 20 phone running the EMUI 9.1.0 operating system reveals source code components which, on information and belief, relate to the Wi-Fi security and threat detection features advertised in Huawei's documentation. For example, the manifest includes at least the following elements of interest: com.huawei.systemmanager_9.1.3.350_900103350_AndroidManifest.xml: <service name="com.huawei.netassistant.wifisecure.WifiSecureService" process=":wifisecure" exported="false"/> -<receiver name="com.***huawei.netassistant.wifisecure.WifiSecureReceiver***" process=":service" exported="false"> -<intent-filter><action name="com.huawei.systemmanager.action.wifisec.notification"/> </intent-filter></receiver> The Huawei eSight and eSight Network further incorporates the WIDS system: Wireless Network Security Detection The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non–Wi-Fi interferences and provides frequency spectrum analysis features. WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices. Huawei eSight Full Product Datasheet, CH 12 eSight WLAN Manager; p. 53 (2013-09-03) Huawei Technologies Co., Ltd.; *see also* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 58-59 (indicating that, on information and belief, all versions of eSight incorporate WIDS). In another non-limiting example, Huawei installed a Wireless local or metropolitan area network at Waichai in Chicago, Illinois using S9700/S6700/S5700/WLAN products: The [Weichai North America] center located in suburban Chicago, which covers 20-acre parcel, and over 300 engineers will be working in this center. … Huawei offered a comprehensive and tailor-made solution for Weichai, which provided end-to-end applications and services based on Huawei products [including] Two clustered S9706 LAN switches stacking with service interfaces at core layer combined with stacked gigabyte access S5700 POE LAN switches to create a loop-free network with high reliability. • High density wireless users access capability and intelligent wireless network The Huawei AP6010 LAN access points provide integrated built-in MIMO antenna and spectrum analysis for even frequency coverage with no coverage hole, concurrent user access rate 20 percents higher than industry average. Moreover, wireless authentication and authorization can provide fine-grained access control for the security of WLAN network. …

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei was chosen as the only vendor by Weichai… … Huawei provided the necessary infrastructure of networks, Unified Communications and Collaboration (UC&C), IT solutions and simplified network management. Huawei In Large Enterprise Case Studies at 12-13 (available at http://www.enterprisesolutions.altech.co.za/sites/.  collab_d7_live/files/Huawei_in_Large_Enterprise%28include%20Small%20Campus%29_1.pdf) HUAWEI WLAN Successful Stories PowerPoint at 2.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei further installed networks at Crowley Independent Schools in Texas: HUAWEI WLAN Successful Stories PowerPoint at 4; *see also* http://support.huawei.com/en/about/media_center/video_clips_list/hw-341648.htm  On information and belief, and as further discovery will show, Huawei has installed networks in other US locations, for example:

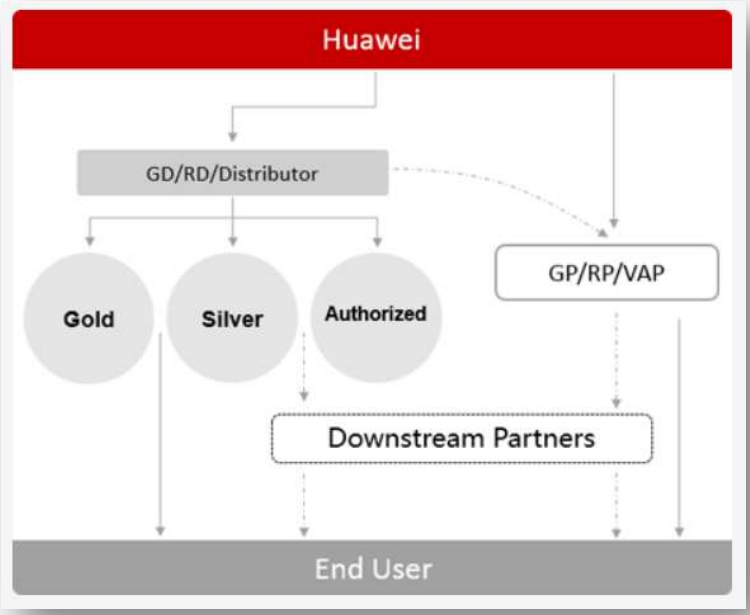
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Sears, one of the leading US retail enterprises, decided to use Huawei's technology and equipment when upgrading the networks of hundreds of stores. Northern Michigan University, Crowley Independent School District in Texas and Digital Domain, a visual effects and digital production company in Hollywood, have adopted storage, Internet solutions and other services provided by Huawei. http://www.globaltimes.cn/content/864994.shtml On information and belief, all Huawei WLAN products, when combined to form a wireless local or metropolitan area network, are able to utilize the WIDS/WIPS technology. Huawei WLAN products are specifically designed to be linked together to form a wireless network, and to be used with other laptops, tablets, phones and WiFi capable devices, and Huawei directs and encourages such conduct. Accordingly, Huawei indirectly infringes this claim by inducing infringement. *See e.g.,* WLAN Installation Service, available at http://support.huawei.com/enterprise/NewsReadAction.action?newType=05&contentId=NEWS1000006056; Enterprise NMS and Application Software Installation Service, available at http://support.huawei.com/enterprise/NewsReadAction.action?newType=05&contentId=NEWS1000006040 and other channel partner service descriptions at https://e.huawei.com/en/partner/partner-program/services In yet a further example, Huawei has a 3, 4 and 5 Star and Global Certified Service Partner Certification program, in which, among other things, allows partners to receive Partner Enablement Support from Huawei. Service partners must meet certain requirements, for example:

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 https://e.huawei.com/en/partner/partner-program/Overview/Standard

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei offers its partners numerous trainings and certificates related to Enterprise Network, including courses that train individuals on designing and deploying WLAN networks, including aspects of WIDS/WIPS and network security. *See, e.g.,* Training Description for Enterprise Network, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/channel%20partner%20program/legal%20-%20commercial/services/learning%20services/hw_201676; *see also* https://e.huawei.com/en/partner/partner-program/apply-for-specialization/network; see also https://e.huawei.com/en/partner/partner-program/Overview/Enablement ("Huawei's Training System Huawei offers a broad variety of training courses such as HALP training, e-learning, and instructor-led courses to help channel partners improve their capabilities.") Huawei has at least 11 service partners that are part of its Enterprise Networking CSP Program, including: Eccom Network(USA) Inc FusionStorm China Telecom (Americas) Corporation Datalink Networks, Inc. Entisys360 Vlan24 Inc CANCOM US UNeed Solutions Inc. dba Noviant MJP Technologies Inc Unified Connexions, Inc. Stellar Services *See* https://e.huawei.com/en/partner/find-a-partner

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei encourages its partners to "promote Huawei's brand in the enterprise business market.":

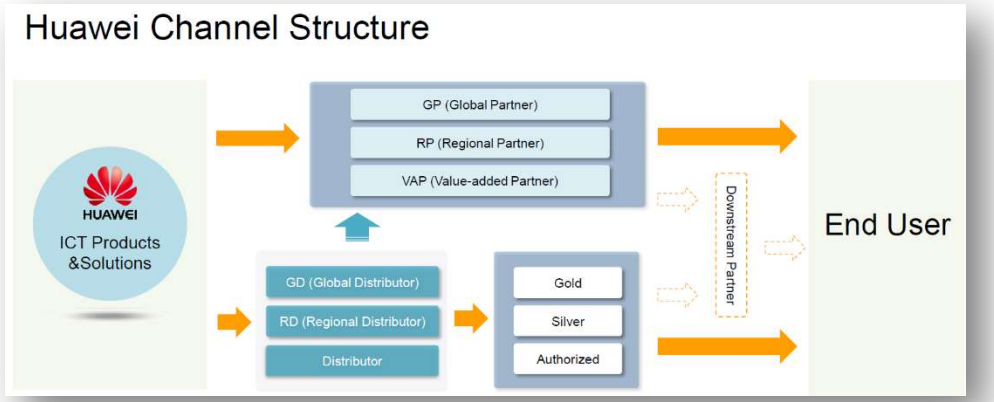


Huawei's Channel Policy Principles

The principle of Huawei's channel policy is "to work and collaborate on a win-win basis."

Work and collaborate: Maximize the value for our channel partners and customers by motivating channel partners to explore the market and promote Huawei's brand in the enterprise business market.

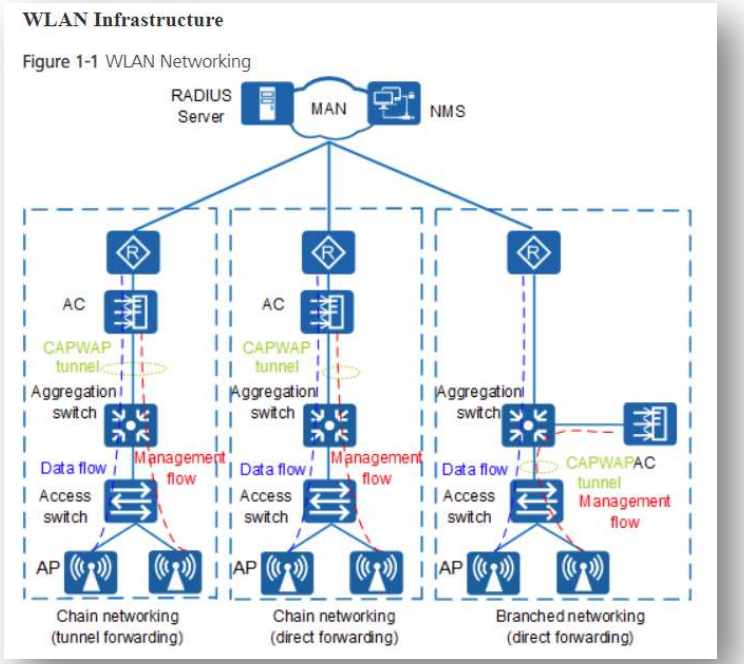
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Classification of Channel Partners Tier1 Partner: Distributor and Value Added Partner (VAP). Distributors include Global Distributors (GDs), Regional Distributors (RDs), and Local Distributors. Global Distributors and Regional Distributors are distributors that run business in multiple countries. Global Partners (GPs) and Regional Partners (RPs) work with Huawei in multiple countries and regions. Tier 2 Partner: Gold Partner, Silver Partner, and Authorized Partner For more information visit our Channel Partner Program page. https://e.huawei.com/en/partner/become-a-partner

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 Distributors must have "3 dedicated employees for Huawei enterprise business" and 6M sales performance thresholds Channel Partner Program Briefing 2018, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204 Further Distributors - Act as major partners of Huawei's Enterprise Business Group (BG) in regional markets. - Promise to accomplish business targets for related products and targets for distribution business. https://e.huawei.com/en/partner/partner-program/policy At least two Huawei Distributors exist in the United States,

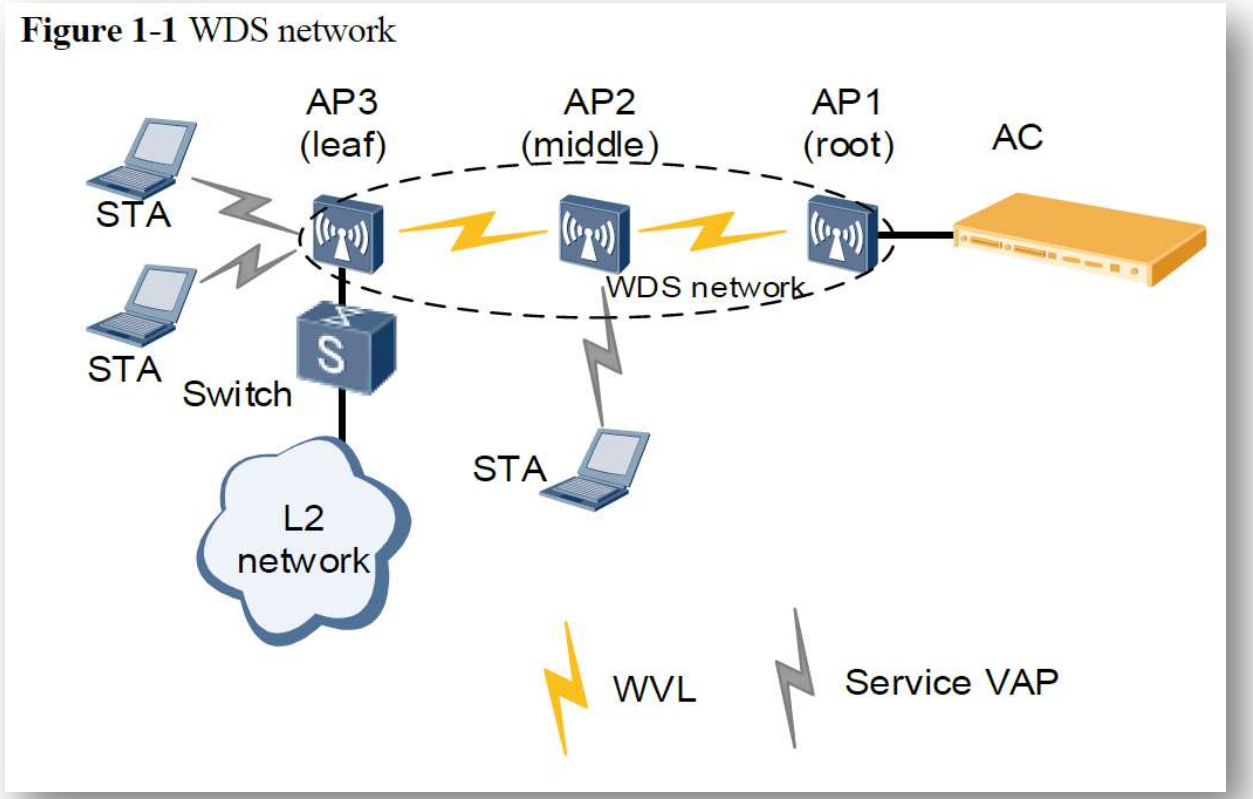
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	ASI Computer Technologies, Inc. in Fremont, CA; (selling Enterprise Cloud Communications, Data Center Switch, IT, Cloud Computing, Transport Network, Security, Access Network, Video Surveillance, Enterprise Networking Common, Campus Switch & WLAN, Enterprise Gateway, Router, UPS, Network Management) Wav, Inc. in Aurora Ill, (selling Data Center Switch, Enterprise Gateway, IT, Cloud Computing, Access Network, Network Management, Video Surveillance, Router, Enterprise Networking Common, Enterprise Cloud Communications, UPS, Campus Switch & WLAN, Transport Network, Security) https://e.huawei.com/en/partner/find-a-partner Value Added Partners must have a 2M sales performance threshold Channel Partner Program Briefing 2018, at p. 6, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204 Value Added Partners: - Act as major partners of Huawei's Enterprise BG in regional markets. - Promise to attain business targets for related industries and customers of Huawei's Enterprise BG. - Develop industry customer relationship platforms and provide support for Huawei's products to industry users. https://e.huawei.com/en/partner/partner-program/policy Value Added Partners in the United States that offer Enterprise Network products include:

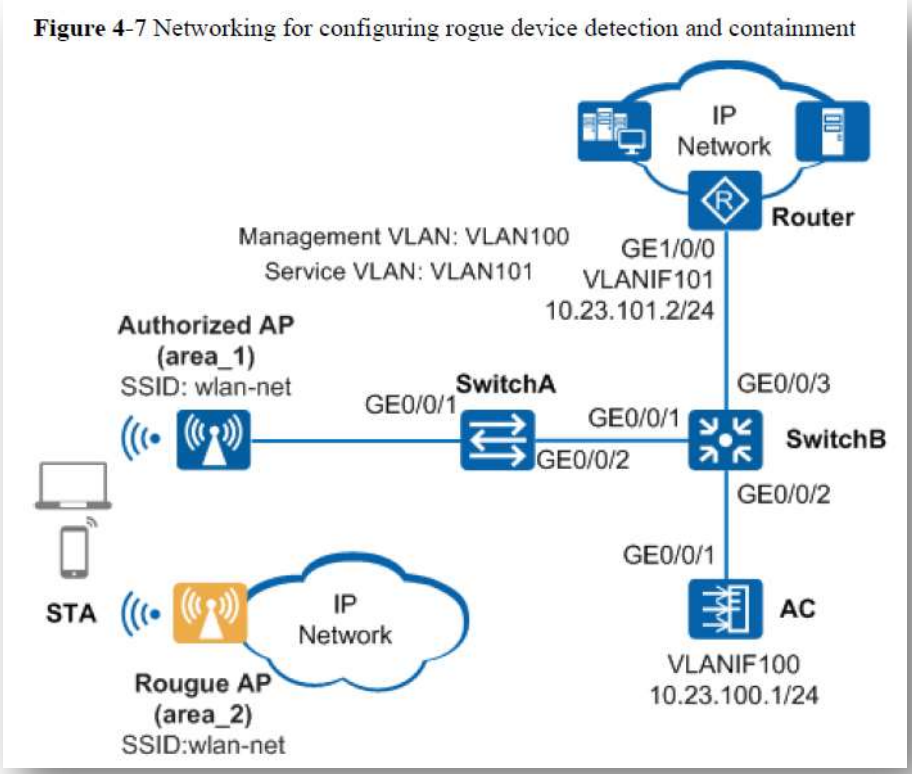
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Proyectos Integrales Solares SL dba Proinso US LLC FusionStorm Consolidated Electrical Distri Rahi Systems, Inc Onesource Distributors, LLC Sonepar Management Us, Inc. CANCOM US WORLD WIDE TECHNOLOGY, LLC Wesco Distribution, Inc. Entisys360 China Telecom (Americas) Corporation *See* https://e.huawei.com/en/partner/find-a-partner Gold Partners in the United States that offer Enterprise Network products include Cloud Trekkers Technologies Inc Silver Partners in the United States that offer Enterprise Network products include Twotrees Technologies, LLC Mark III Systems, Inc UNeed Solutions Inc. dba Noviant Gold and Silver Partners have sales performance thresholds of 0.5M and 0.25M (Channel Partner Program Briefing 2018, at p. 6, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Gold and Silver Partners - Act as major partners of Huawei's Enterprise BG in regional markets. - Promise to accomplish business targets for related industries and customers of Huawei's Enterprise BG. - Develop industry customer relationship platforms and provide support for Huawei's products to industry users. https://e.huawei.com/en/partner/partner-program/policy Huawei also has more than 50 Authorized Partners that offer Enterprise Network products *See* https://e.huawei.com/en/partner/find-a-partner Huawei further actively encourages infringement and sales of Huawei networks by imposing penalties for violations: "Level-2 violation" of the partnership agreement to "direct unauthorized sales" "Level-3 violation" for "indirect unauthorized sales" and if a "Channel does not fulfill service contract or order" or "Provides services to customers through non-Huawei certified maintenance companies" Channel Partner Program Briefing 2018 at p.9, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204

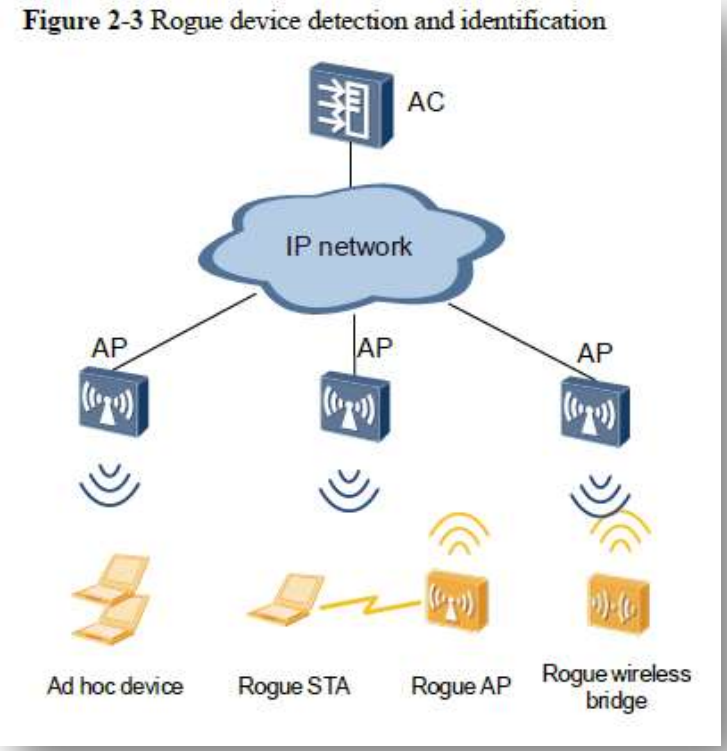
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
[a] a plurality of stations for transmitting data therebetween using a media access layer (MAC), each of said stations having a respective MAC address associated therewith; and	Huawei '678 Patent Accused Products form a network comprising a plurality of stations (including, without limitation, Stations, STAs, Access Points, APs, and/or Remote Units) for transmitting data therebetween using a media access layer (MAC), each of said stations having a respective MAC address associated therewith. One exemplary network configuration is shown: 

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	As shown in Figure 1-1, a WLAN consists of access points (APs), PoE switches, access controllers (ACs), Remote Authentication Dial In User Service (RADIUS) server, and network management system (NMS). - AP: WLAN access device. Huawei provides a series of fit APs to meet indoor and outdoor networking requirements. - PoE switch: upstream devices for APs. It provides data switching and power for APs. If only one AC is required and the AC has PoE ports, the PoE switch is not required. - AC: manages APs and controls the rights of WLAN users. - RADIUS server: authenticates WLAN users and assigns rights to them. The RADIUS server is installed on the SPES server. - NMS: manages APs and ACs. It monitors status of ACs and APs in real time, processes alarms, and analyzes data. HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 2. https://support.huawei.com/enterprise/en/doc/EDOC1000184389/1d542042/introduction-to-wlan In another configuration example, a WDS (Wireless Distribution System) may wirelessly connect two WLANs:

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 Huawei Technologies Co., Ltd. WLAN WDS Technology White Paper Issue 03 (2017-11-21) at 1-2.

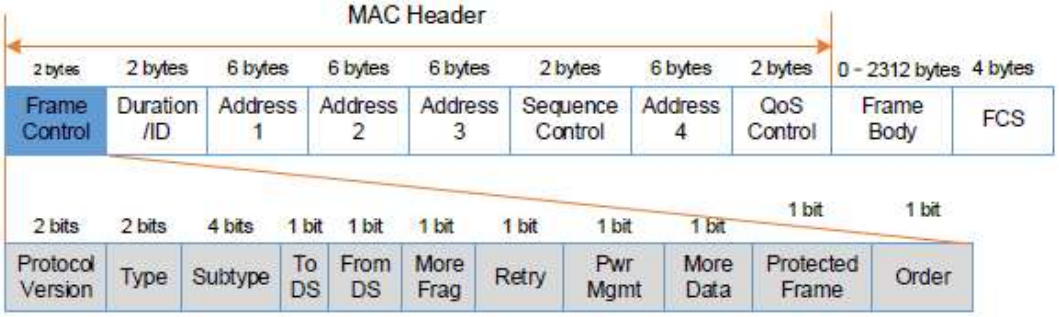
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	See also:  **Figure 4-7** Networking for configuring rogue device detection and containment IP Network Router Management VLAN: VLAN100 Service VLAN: VLAN101 GE1/0/0 VLANIF101 10.23.101.2/24 Authorized AP (area_1) SSID: wlan-net GE0/0/1 SwitchA GE0/0/1 GE0/0/3 SwitchB GE0/0/2 GE0/0/2 GE0/0/1 STA IP Network AC VLANIF100 10.23.100.1/24 Rougue AP (area_2) SSID:wlan-net HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 123.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows: 1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios. 2. The AC delivers the configuration to the AP. 3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames: − Beacon − Association Request − Association Response − Reassociation Request − Reassociation Response − Probe Response − Data frame 4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 2-3 Rogue device detection and identification  The AP identifies the types of neighboring wireless devices based on detected 802.11 management and data frames. The **Frame Control** field in the MAC header of a frame indicates the frame type. Figure 2-4 shows the subfields of the **Frame Control** field.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION

Figure 2-4 MAC header of an 802.11 frame



Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 5.

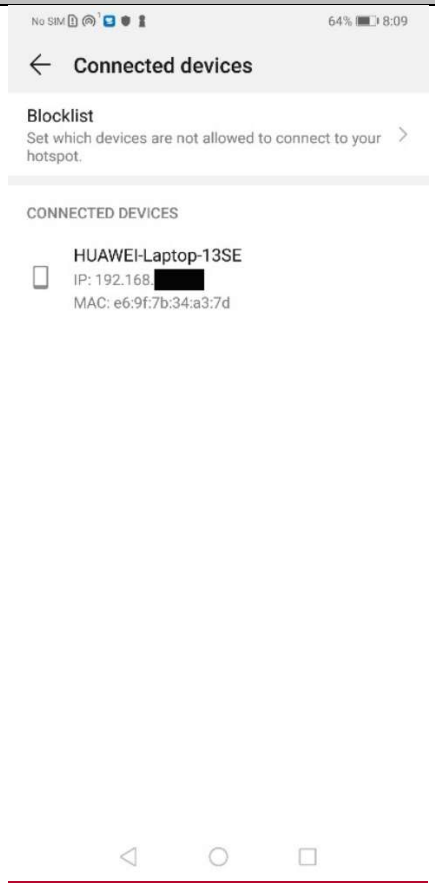
Each station has a MAC address associated therewith

Attribute	Description
MAC address	MAC address of the device

Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 9.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	MAC address - A link layer address or physical address. It is six bytes long. *See e.g.,* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at 253. Huawei consumer devices, including laptops, phones and tablets, also participate in the WIDS system as client stations (also referred to in WIDS and documentation as "STAs" or "ad hoc" devices). *See, e.g.*, Huawei Technologies Co., Ltd., *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 7 ("When receiving a Probe Request, an Association Request, or a Reassociation Request frame, the AP determines whether the sender is an ad hoc device or STA based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame") *see also id.* at 11 ("Rogue STAs: After detecting a rogue STA, a monitor AP uses the BSSID and MAC address of the rogue STA to send a fake unicast Deauthentication frame to contain it. A STA whitelist can also be configured to prevent STAs in the STA whitelist from associating with rogue APs"). Huawei consumer devices, including laptops, phones and tablets, transmit and receive data using a MAC address associated with the device. For example, a Huawei Matebook 13 SE laptop and a Huawei Mate 20 phone both purchased in the United States each have a MAC address associated therewith, and use that MAC address in communications over Wi-Fi networks:

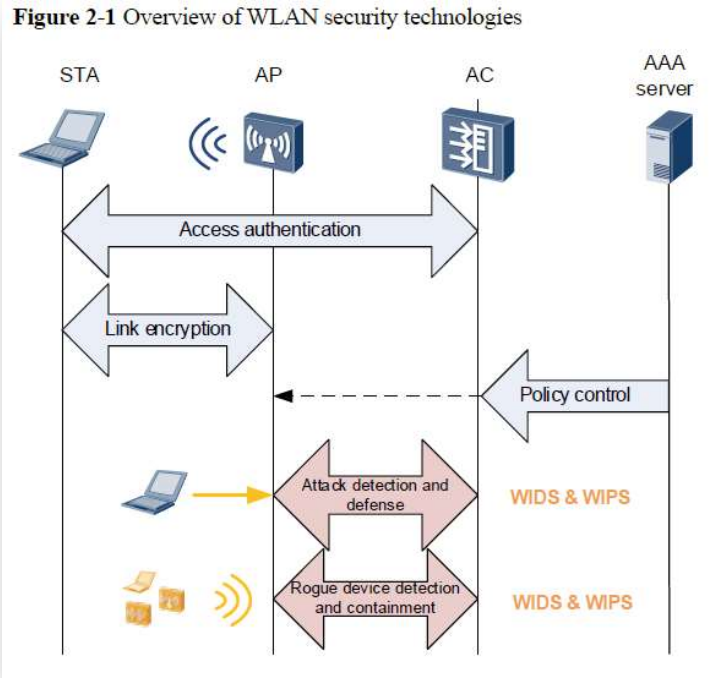
***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

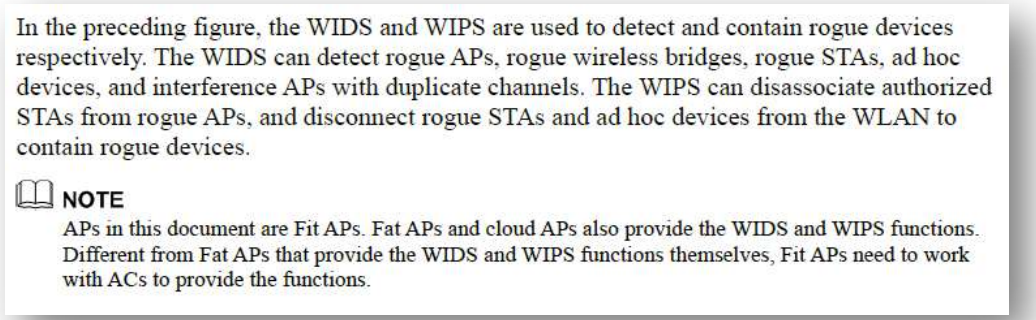
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	

'678 PATENT CLAIM 12	**INFRINGEMENT BY HUAWEI CORPORATION**
[b] a policing station for detecting intrusions into the wireless network by	Huawei '678 Patent Accused Products comprise a policing station for detecting intrusions into the wireless network. For example, Huawei WLAN products utilize the WIDS technology to detect intrusions > 802.11 networks are open wireless public networks, and vulnerable to various threats caused by unauthorized APs and STAs, ad hoc networks, bogus APs, and denial of service (DoS) attacks of malicious STAs. The Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions monitor and prevent the preceding attacks on WLANs. > This document describes WIDS and WIPS technologies used by Huawei WLAN products. Enterprises can use the WIDS and WIPS functions to secure their wireless networks, reduce interference from unauthorized devices, protect STAs from malicious attacks, and deliver better user experience. > … > The WIDS detects rogue STAs, malicious user attacks, and wireless network intrusions. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 1-2. > The WIDS and WIPS functions of Huawei WLAN products ensure security of customers' wireless networks, reduce interference from rogue devices, and protect STAs from malicious attacks, delivering better user experience. > • Selection of different protection measures based on their network scale

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	The WIDS and WIPS functions provide different protection measures based on the scale of customer networks. - For home networks or small enterprise networks, protection measures are provided to control access of APs and STAs using blacklists and whitelists. - For small- and medium-scale enterprise networks, WIDS attack detection and defense are provided. - For medium- and large-scale enterprise networks, rogue device detection, identification, defense, and containment are provided. Customers can also perform other protection configurations. ● Rogue device identification and defense The WIDS and WIPS functions can identify rogue devices on the WLAN and take preventive measures to protect customer networks against intrusions or interference of rogue devices. ● Customer network protection against attacks The WIDS and WIPS functions can detect multiple types of attacks such as flood attacks, weak IV attacks, spoofing attacks, brute force WPA/WPA2/WAPI PSK cracking, and WEP shared key cracking. The functions protect customer networks from being attacked by rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 20. For example, a monitor AP may act as a policing station for detecting intrusions (e.g., rogue devices) into the wireless network:

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 In the preceding figure, the WIDS and WIPS are used to detect and contain rogue devices respectively. The WIDS can detect rogue APs, rogue wireless bridges, rogue STAs, ad hoc devices, and interference APs with duplicate channels. The WIPS can disassociate authorized STAs from rogue APs, and disconnect rogue STAs and ad hoc devices from the WLAN to contain rogue devices. NOTE APs in this document are Fit APs. Fat APs and cloud APs also provide the WIDS and WIPS functions. Different from Fat APs that provide the WIDS and WIPS functions themselves, Fit APs need to work with ACs to provide the functions. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3. 2.2 Rogue Device Detection Rogue device detection of WLANs is enabled to monitor the entire network. Monitor APs are deployed on a WLAN that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless signals to detect rogue devices. 2.2.1 Working Modes of APs Before enabling rogue device detection on a WLAN, configure APs' working modes. An AP works in normal or monitor mode. • Normal mode: If the WIDS and WIPS functions and other air interface scan functions are disabled on a radio, such as spectrum analysis and STA location, this radio can be used only to transmit common WLAN service data. If the WIDS and WIPS functions

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION

are enabled, the working mode of the radio is automatically switched to hybrid. In addition to transmitting common WLAN service data, the radio can also provide the monitoring function. In this case, transmission of common WLAN service data is affected.

- Monitor mode: A monitor AP scans devices on the WLAN and listens on all 802.11 frames on wireless channels. In this case, the monitor AP provides only the monitoring function and cannot transmit WLAN service data.

The following figure shows the principles of the two working modes.

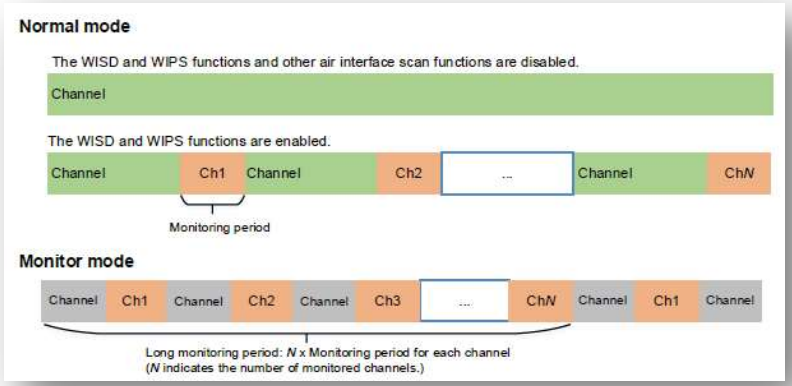
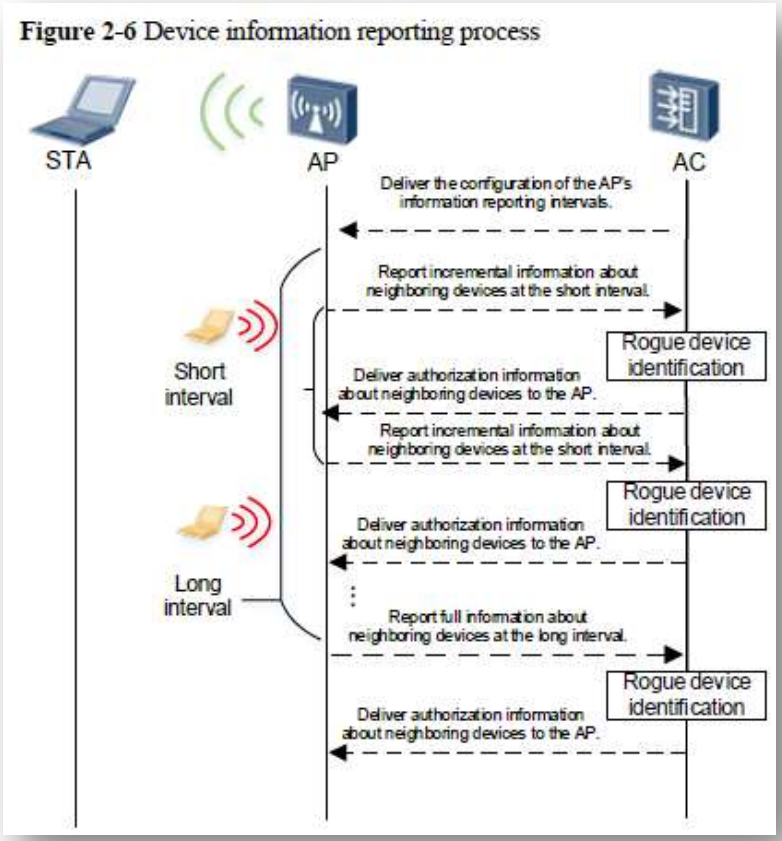


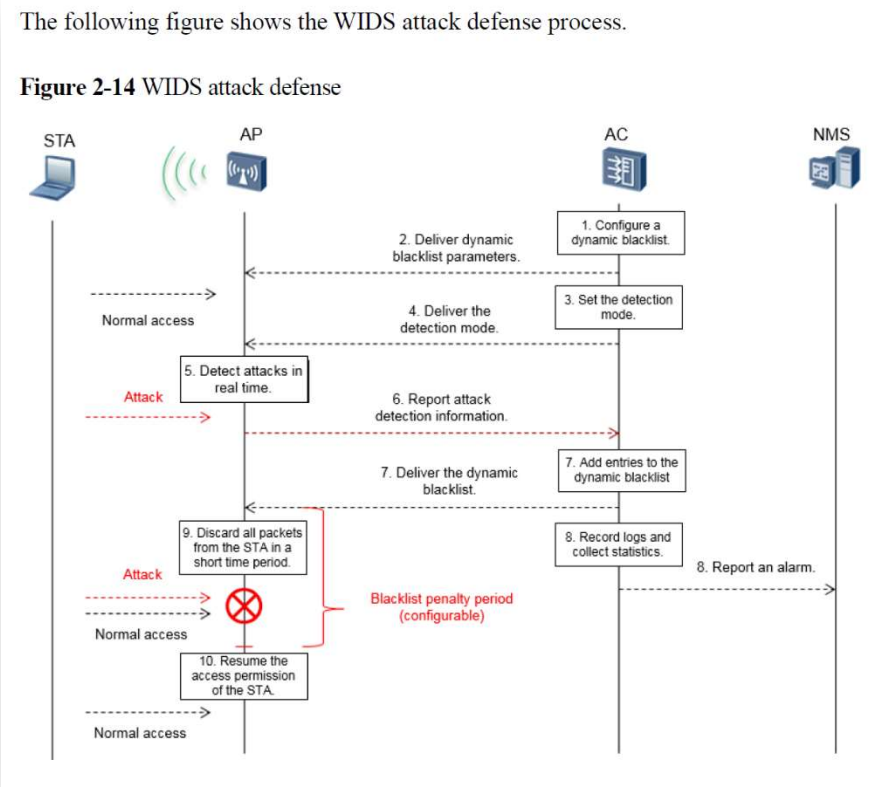
Figure 2-2 Principles of the two working modes

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION

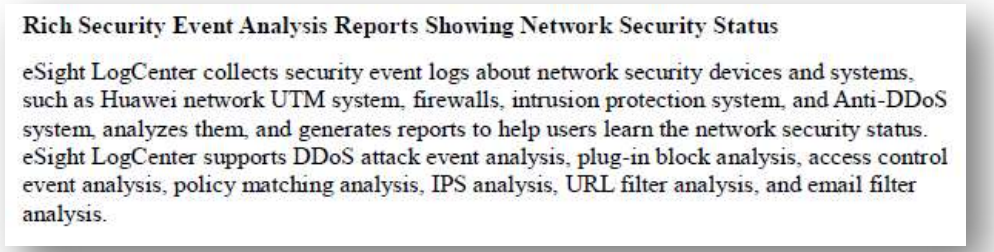


Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3-4.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	The device information reporting process is described as follows: • On the AC, a short interval is configured for the AP to report information about neighboring wireless devices. (The long interval is provided by the system by default.) • The AC delivers the configuration to the AP. • The AP listens on frames to collect information about neighboring wireless devices, and reports the information to the AC at the specified short interval. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC. • The AP reports full information about all detected wireless devices to the AC at the long interval for information synchronization. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 8.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	The following figure shows the WIDS attack defense process. **Figure 2-14** WIDS attack defense  Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 17.

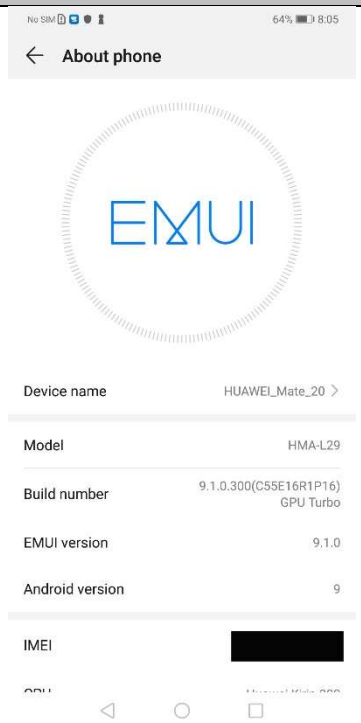
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	The Huawei eSight Platform, including at least the WLAN Manager and LogCenter Manager, is further used as a network management system that also detects intrusions into the wireless network**:** The Huawei eSight Platform further incorporates the WIDS system: Wireless Network Security Detection The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non–Wi-Fi interferences and provides frequency spectrum analysis features. WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices. Huawei eSight Full Product Datasheet, CH 12 eSight WLAN Manager; p. 53 (2013-09-03) Huawei Technologies Co., Ltd.; *see also* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 58-59 (indicating that, on information and belief, all versions of eSight incorporate WIDS).

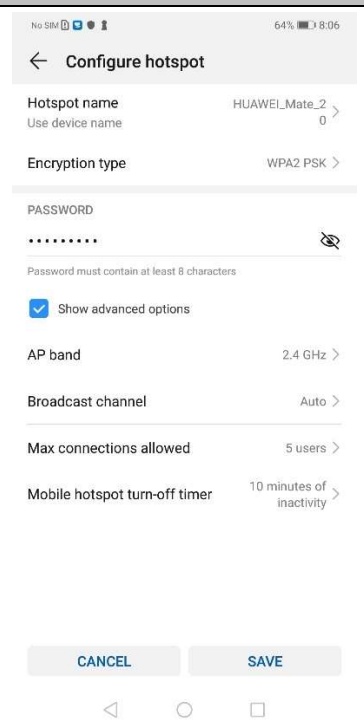
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 **Rich Security Event Analysis Reports Showing Network Security Status** eSight LogCenter collects security event logs about network security devices and systems, such as Huawei network UTM system, firewalls, intrusion protection system, and Anti-DDoS system, analyzes them, and generates reports to help users learn the network security status. eSight LogCenter supports DDoS attack event analysis, plug-in block analysis, access control event analysis, policy matching analysis, IPS analysis, URL filter analysis, and email filter analysis. Huawei eSight Full Product Datasheet, CH 11 eSight LogCenter Manager; p. 44 (2013-09-03) Huawei Technologies Co., Ltd. Security Users can monitor rogue devices, clients, interference sources, and attacks on the network, define rules to identify intrusion devices, generate remote alarm notifications, and take measures to prevent intrusions. 1. Supports statistics and display of and countermeasure against rogue devices. 2. Supports the display of and countermeasure against rogue clients and suppression access protection. 3. Supports statistics and display of non-Wi-Fi interference sources. 4. Supports statistics and display of attacks and protection against attacks. 5. Allows users to define rules and classify rogue APs (rogue, suspected-rogue, adjacent, suspected-adjacent, and interference). Supported rule matching indicators include

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	adjacent- or same-frequency interference, signal strength, SSID (fuzzy match/regular expression), the number of detected APs, and whether to attack. eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 63. On information and belief Huawei consumer devices, including laptops, phones and tablets also can participate in the WIDS system as access points ("APs"), including when configured as a mobile hotspot. For example, a Huawei Matebook 13 SE laptop and a Huawei Mate 20 phone both purchased in the United States allow configuration as, can operate as, and can connect to the other as, a mobile WiFi Hotspot:

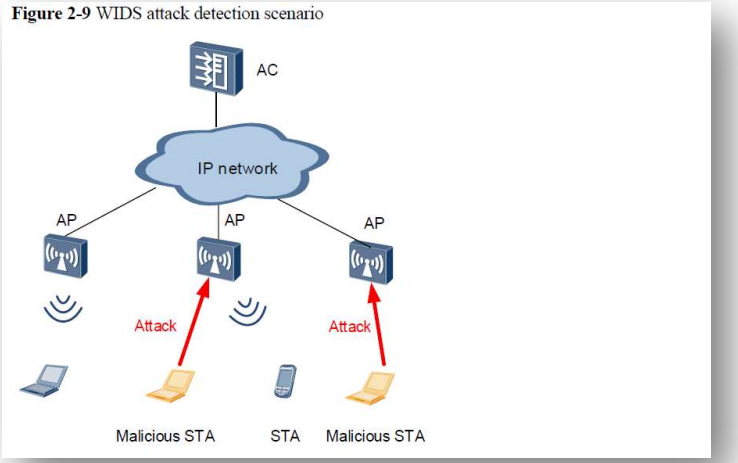
***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION





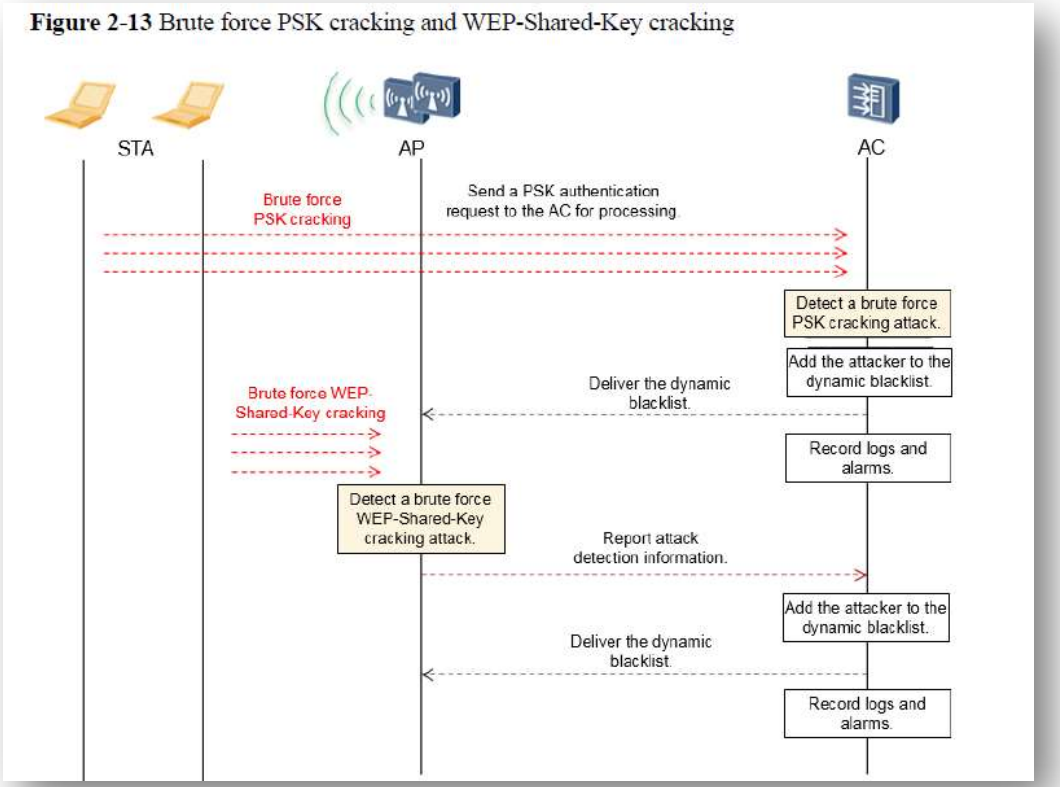
Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also implement intrusion detection according to the claim. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
[c] monitoring transmissions among said plurality of stations to detect failed attempts to authenticate MAC addresses; and	The '678 Patent Accused Products comprise policing stations, as described above in [b], that are capable of monitoring transmissions among said plurality of stations to detect failed attempts to authenticate MAC addresses. For example, the policing station is capable of detecting when an intruder attempts to authenticate a MAC address using Brute Force Cracking in which there are failed attempts to authenticate. 2.4 WIDS Attack Detection To protect a WLAN against attacks, you can configure real-time attack detection on APs. When detecting abnormal behavior or packets, the system considers that it is attacked and performs automatic security protection. **Figure 2-9** WIDS attack detection scenario 

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	On the WLAN shown in the preceding figure, WIDS attack detection can be enabled on the AC when the WLAN access service is provided. The WIDS can detect 802.11 flood attacks, spoofing attacks, and weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12. 2.4.4 Defense Against Brute Force Cracking A brute force attack, or exhaustive key search, is a cryptanalytic attack that tries every possible password combination to find the real password. For example, a password that contains only four digits may have a maximum of 10,000 combinations. The password can be cracked after a maximum of 10,000 attempts. Theoretically, an attacker can use the brute force method to crack any password. The cracking duration varies depending on the security mechanism and password length. Therefore, brute force cracking threats exist when any authentication mode is used. ● When a WLAN uses the WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key security policy (link authentication), attackers may use the brute force method to crack passwords. ● When a user authentication mode is used, such as MAC address, Portal, or 802.1X authentication, brute force cracking threats also exist. Huawei Technologies Co., Ltd. WLAN WIDS & WIPS Technology White Paper; Issue 2.0 (2017-07-05) at 15.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION

Figure 2-13 Brute force PSK cracking and WEP-Shared-Key cracking



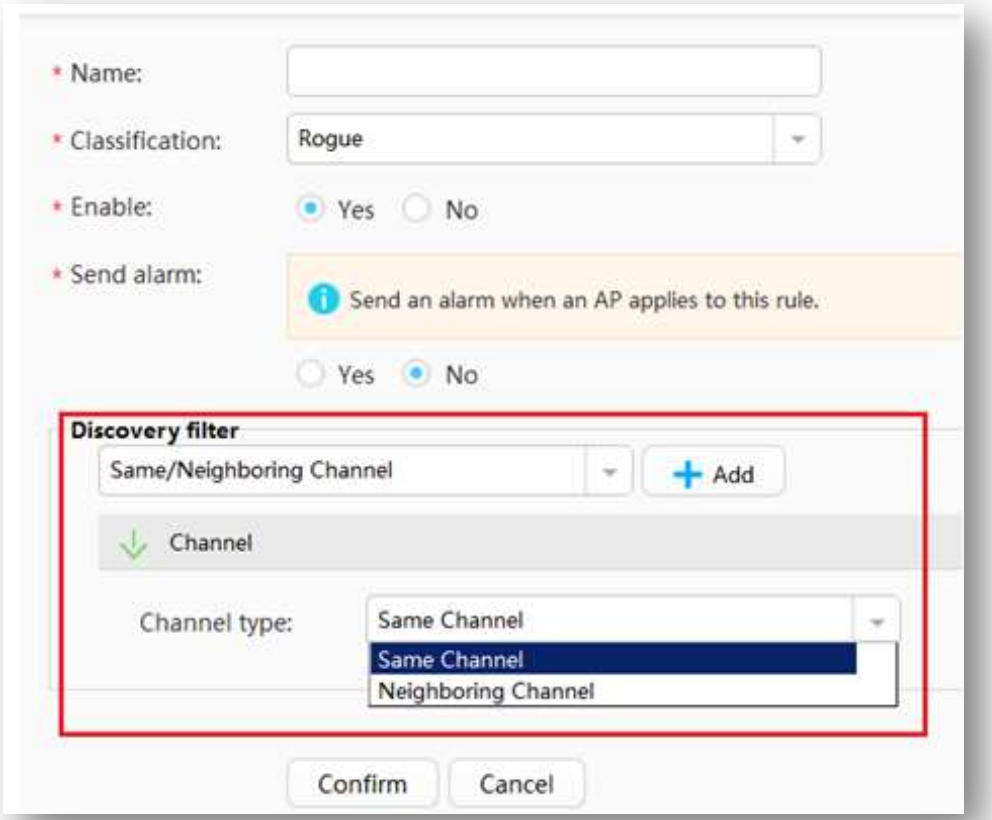
When different user access authentication modes are used, such as MAC address, Portal, and 802.1X authentication, defense against brute force cracking is also needed. The basic principle is similar, which is described as follows:

- MAC address authentication: The MAC address of a STA is used as an account and sent to the RADIUS server for authentication. If authentication fails, the STA is added

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	to the STA blacklist and prohibited from accessing the network within a short time period (configurable and 60s by default). Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 16. The Huawei eSight Platform further incorporates the WIDS system and monitors transmissions among the stations as indicated above. Wireless Network Security Detection The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non–Wi-Fi interferences and provides frequency spectrum analysis features. WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices. Huawei eSight Full Product Datasheet, CH 12 eSight WLAN Manager; p. 53 (2013-09-03) Huawei Technologies Co., Ltd.; *see also* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 58-59 (indicating that, on information and belief, all versions of eSight incorporate WIDS). WIDS Wireless Intrusion Detection System The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security.

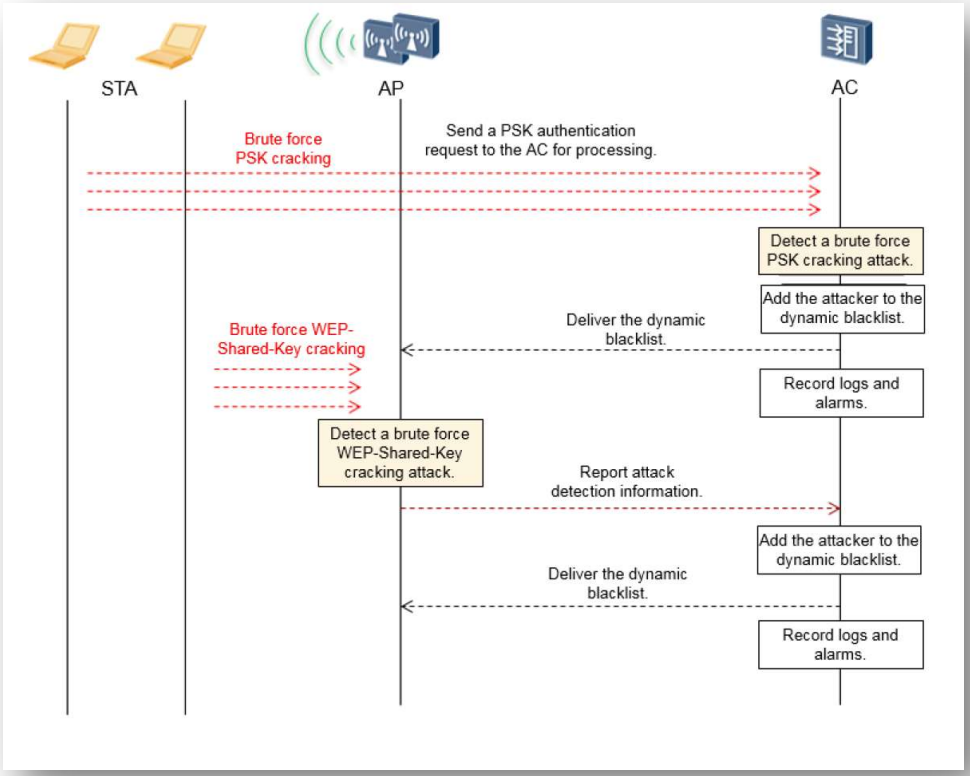
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	… Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. Same or adjacent channel This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12. On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for failed MAC address authentications, including when configured as a mobile hotspot.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also monitor for failed MAC address authentications. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").
[d] generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.	As described above, on information and belief, the policing stations are capable of generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address. For example, if the AP considers that the STA is using the brute force cracking, it generates and sends an alarm to the AC, and on information and belief, such alarm is generated in the event of a MAC address brute force cracking attempt: An AP checks whether the number of key negotiation attempts within a specified time period during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the specified threshold (configurable). If so, the AP considers that the STA is using the brute force method to crack the password and reports an alarm to the AC. … When different user access authentication modes are used, such as MAC address, Portal, and 802.1X authentication, defense against brute force cracking is also needed. The basic principle is similar, which is described as follows: • MAC address authentication: The MAC address of a STA is used as an account and sent to the RADIUS server for authentication. If authentication fails, the STA is added to the STA

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	blacklist and prohibited from accessing the network within a short time period (configurable and 60s by default). Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 15-16. Defense against PSK cracking: Security authentication modes for wireless users include WEP shared key, WPA/WPA2 PSK, WPA/WPA2 dot1x, WAPI certificate, and WAPI PSK. Theoretically, if a client keeps exhaustive key search, it can crack the key. Therefore, a protection mechanism is added so that when the number of authentication attempts exceeds a specified threshold, packets from the client are discarded in a specified time to prevent the user from continuous brute force attacks, reducing the adverse effects of frequent negotiations on devices and the network. WLAN WIDS Technology White Paper, Issue 1.0 (2014-04-24) at 12.

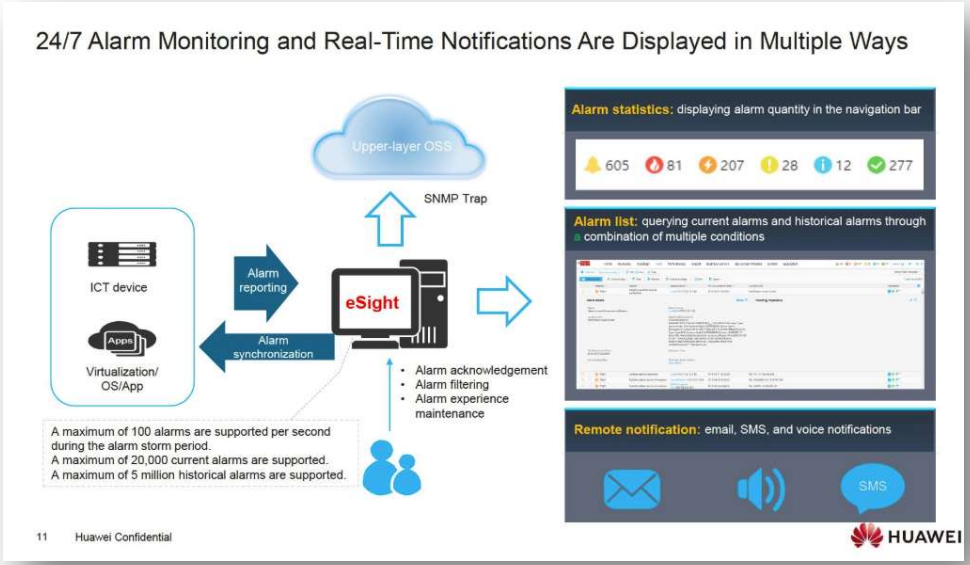
'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	 Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 16.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	As described in Huawei Support documentation, a number of failed attempts to authenticate the MAC address results in locking the user account, which, on information and belief, triggers the generation of an alarm as described above: > By default, the account locking function is enabled on the AC to ensure security of user passwords. If a user fails authentication over 30 times within 30 minutes, the AC locks the user account for a specified period of time, during which this account cannot be authenticated. > Some terminals initiate MAC address authentication but do not initiate Portal authentication several times after associating with SSIDs. (For example, background applications on a mobile phone initiate multiple TCP requests instantly after the mobile phone associates with an SSID.) If the MAC address of a terminal is not recorded in the AAA server, and the terminal fails authentication over 30 times within 30 minutes, the AC locks the user account (the terminal's MAC address). Therefore, the terminal fails MAC address authentication and the Portal authentication page is displayed. Huawei Community Forums, [From Beginner to Expert - WLAN Fundamentals] Section 11 - WLAN Access Authentic. Jun 25, 2016 (at https://forum.huawei.com/enterprise/en/From-Beginner-to-Expert-WLAN-Fundamentals-Section-11-WLAN-Access-Authentic/thread/346361-869) Further, eSight generates an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address, including by utilizing WIDS as described above; further, rogue devices may trigger alarms. For example: > Security > Users can monitor rogue devices, clients, interference sources, and attacks on the network, define rules to identify intrusion devices, generate remote alarm notifications, and take measures to prevent intrusions.

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	1. Supports statistics and display of and countermeasure against rogue devices. 2. Supports the display of and countermeasure against rogue clients and suppression access protection. 3. Supports statistics and display of non-Wi-Fi interference sources. 4. Supports statistics and display of attacks and protection against attacks. 5. Allows users to define rules and classify rogue APs (rogue, suspected-rogue, adjacent, suspected-adjacent, and interference). Supported rule matching indicators include adjacent- or same-frequency interference, signal strength, SSID (fuzzy match/regular expression), the number of detected APs, and whether to attack. eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 63; *see also id.* at 74 (3. eSight supports alarms about communications, environments, rogue devices, non-Wi-Fi interference sources, and attacks to help users locate and resolve faults.).

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION



eSight Overview Presentation at 11.

On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on monitoring for failed MAC address authentications, including when configured as a mobile hotspot.

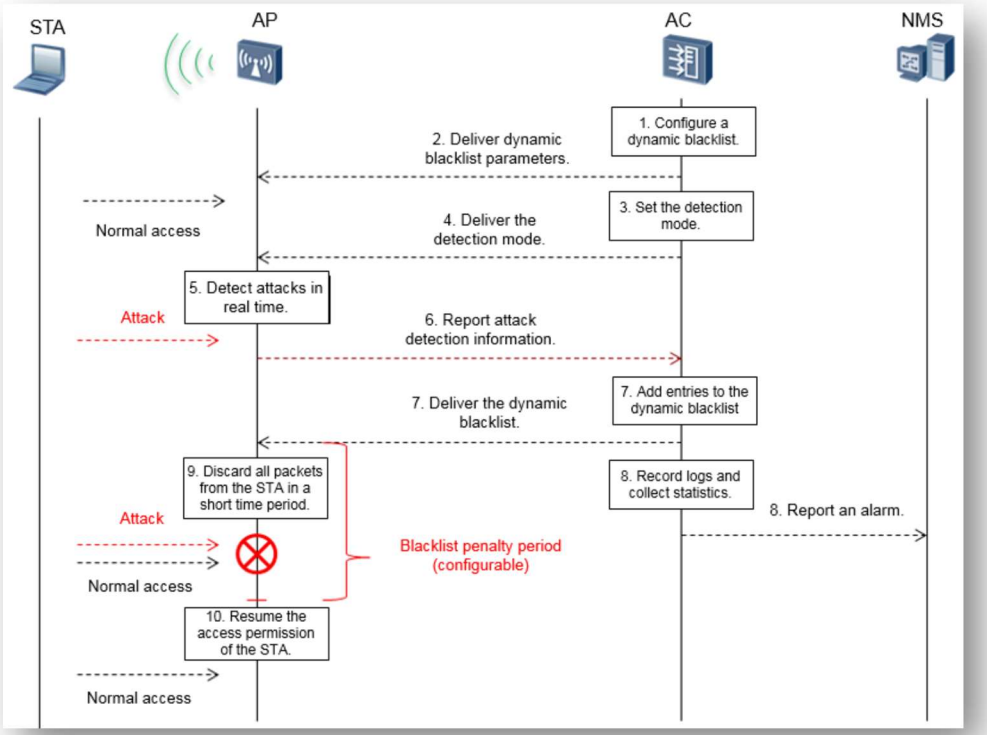
Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also generate an intrusion alert based on monitoring for failed MAC address authentications. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be

'678 PATENT CLAIM 12	INFRINGEMENT BY HUAWEI CORPORATION
	authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION
13. The wireless network of claim 12 wherein said policing station generates an intrusion alert based upon detecting the number of failed attempts to authenticate the MAC address within a predetermined period.	The Huawei '678 Accused Products infringe this claim. *See* Claim 12. Such Instrumentalities further have a policing station capable of generating an intrusion alert based upon detecting the number of failed attempts to authenticate the MAC address within a predetermined period. For example, as described in the WIDS Technology White Paper, on information and belief, an alarm is generated from the AP after a threshold number of authentication attempts: > An AP checks whether the number of key negotiation attempts within a specified time period during [] authentication exceeds the specified threshold (configurable). If so, the AP considers that the STA is using the brute force method to crack the password and reports an alarm to the AC. > … > When different user access authentication modes are used, such as MAC address, Portal, and 802.1X authentication, defense against brute force cracking is also needed. The basic principle is similar, which is described as follows: > ● MAC address authentication: The MAC address of a STA is used as an account and sent to the RADIUS server for authentication. If authentication fails, the STA

'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION
	is added to the STA blacklist and prohibited from accessing the network within a short time period (configurable and 60s by default). Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 15-16. Further, a detection period and detection threshold may be set that, on information and belief, would include the failed attempts to authenticate the MAC address:

'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION



1. The dynamic blacklist function is configured on the AC and the blacklist entry aging time is specified.

2. The AC sends the dynamic blacklist enabled flag and blacklist entry aging time to the AP.

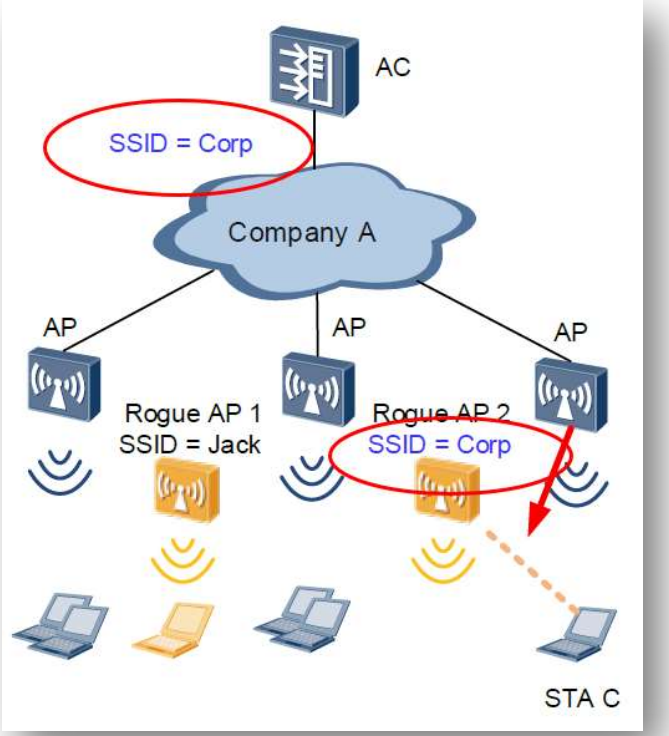
'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION
	3. The WIDS attack detection mode is configured on the AC. The detection period and detection threshold (number of packets detected within the specified time period to identify an attack) are set. 4. The AC delivers the detection mode, detection period, and detection threshold to the AP. 5. The AP detects attacks in attack detection mode delivered by the AC. 6. When the AP detects an attack, it reports attack information to the AC, such as the MAC address of the attacking device and the attack type. After receiving the attack information, the AC adds the attacking device to the attacking device list. If the AP detects no attack from this attacking device in the next three attack detection periods, it requests the AC to delete the attacking device from the list. 7. The AC determines whether to add the attacking device to the dynamic blacklist. It records detected brute force PSK crackers to the dynamic blacklist cache table, and delivers the table to the AP. 8. The AC collects statistics on attack types and sends trap messages to report the attack types to the NMS. 9. After receiving the dynamic blacklist, the AP discards the packets from the attacking devices in the dynamic blacklist. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 17. As described in Huawei Support documentation, for example, the AC may also detect the number of failed attempts to authenticate the MAC address (e.g., over 30 times) within a predetermined period (e.g.,

'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION
	within 30 minutes) which, on information and belief, triggers the generation of an alarm or intrusion alert as described above: > By default, the account locking function is enabled on the AC to ensure security of user passwords. If a user fails authentication over 30 times within 30 minutes, the AC locks the user account for a specified period of time, during which this account cannot be authenticated. > Some terminals initiate MAC address authentication but do not initiate Portal authentication several times after associating with SSIDs. (For example, background applications on a mobile phone initiate multiple TCP requests instantly after the mobile phone associates with an SSID.) If the MAC address of a terminal is not recorded in the AAA server, and the terminal fails authentication over 30 times within 30 minutes, the AC locks the user account (the terminal's MAC address). Therefore, the terminal fails MAC address authentication and the Portal authentication page is displayed. Huawei Community Forums, [From Beginner to Expert - WLAN Fundamentals] Section 11 - WLAN Access Authentic. Jun 25, 2016 (at https://forum.huawei.com/enterprise/en/From-Beginner-to-Expert-WLAN-Fundamentals-Section-11-WLAN-Access-Authentic/thread/346361-869) eSight is also involved in the generation of intrusion alerts, for example: > Security > Users can monitor rogue devices, clients, interference sources, and attacks on the network, define rules to identify intrusion devices, generate remote alarm notifications, and take measures to prevent intrusions. > 1. Supports statistics and display of and countermeasure against rogue devices.

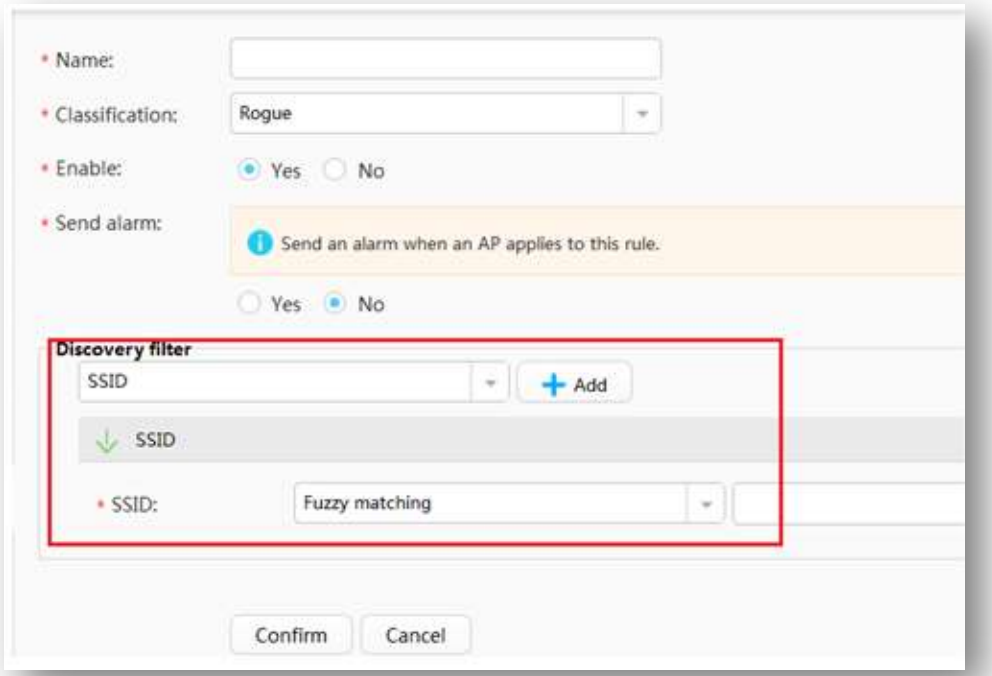
'678 PATENT CLAIM 13	INFRINGEMENT BY HUAWEI CORPORATION
	2. Supports the display of and countermeasure against rogue clients and suppression access protection. 3. Supports statistics and display of non-Wi-Fi interference sources. 4. Supports statistics and display of attacks and protection against attacks. 5. Allows users to define rules and classify rogue APs (rogue, suspected-rogue, adjacent, suspected-adjacent, and interference). Supported rule matching indicators include adjacent- or same-frequency interference, signal strength, SSID (fuzzy match/regular expression), the number of detected APs, and whether to attack. eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 63; *see also id.* at 74 (3. eSight supports alarms about communications, environments, rogue devices, non-Wi-Fi interference sources, and attacks to help users locate and resolve faults.). *See also* claim element 12(d) above.

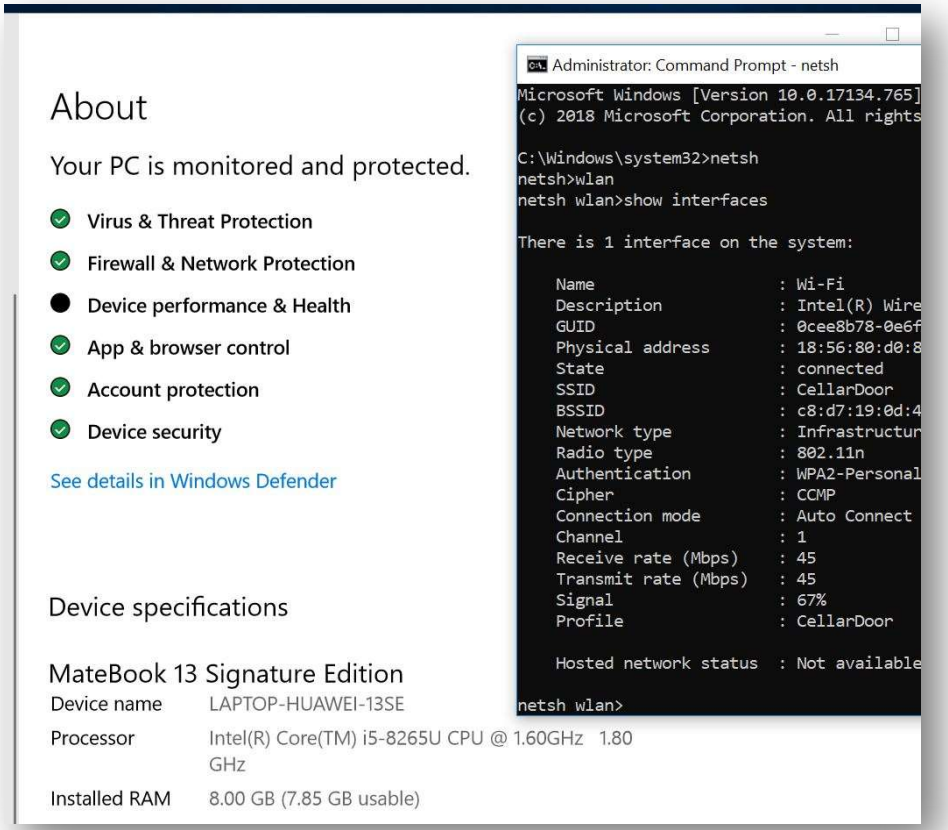
'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
17. The wireless network of claim 12 wherein the wireless network has at least one service set identification (ID) associated therewith; and wherein said policing station	The Huawei '678 Accused Products infringe this claim. *See* Claim 12. Further, the wireless network has at least one service set identification (ID) associated therewith. Most wireless networks have an SSID associated therewith. As a non-limiting example, as described in the WIDS and WIPS whitepaper, a company WLAN may have an associated SSID:

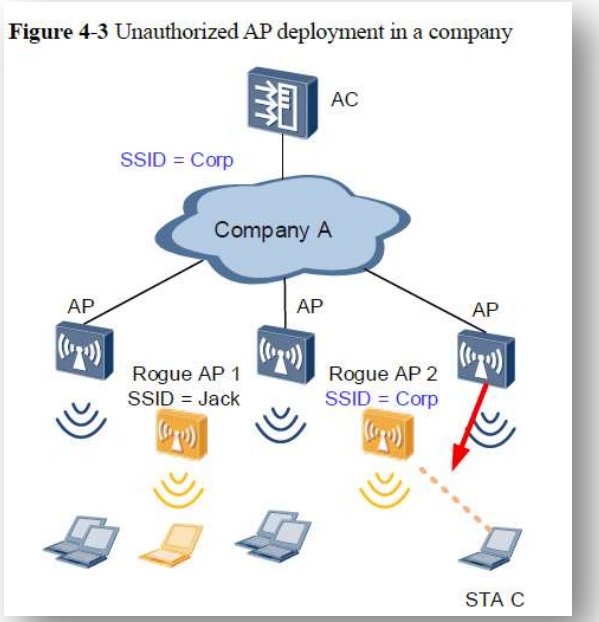
'678 PATENT CLAIM 17	**INFRINGEMENT BY HUAWEI CORPORATION**
further detects intrusions into the wireless network by:	In this case, company B can add the SSID of company A's WLAN to the SSID whitelist so that APs in company A will not be detected as rogue devices… Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 22. 3.1.9 SSID Profile SSIDs identify different wireless networks. When you search for available wireless networks on your laptop, the displayed wireless network names are SSIDs. An SSID profile is used to configure the SSID name and other access parameters of a WLAN. HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 24.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 …Rogue AP 2 uses the same SSID as the WLAN system of the company…

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 22-23 (emphasis added). As further described in the eSight documentation, eSight using WIDS also detects intrusions in the wireless network in accordance with the claim as described below WIDS Wireless Intrusion Detection System The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security. … Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. SSID The service set identifiers of networks from unauthorized vendors or wireless networks established by individuals are similar to authorized SSIDs. For example, the SSIDs are the same or characters are similar (such as 0 and o). In this case, users may be deceived to log in to rogue wireless networks. An SSID rule can be used to detect rogue APs whose SSIDs are similar to the authorized SSIDs or when a specified rule (regular expression) is met.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12. Huawei consumer devices, including laptops, phones and tablets, also use SSIDs and BSSIDs associated with wireless networks. For example, Huawei laptops and tablets such as the Matebook 13 associate SSIDs and BSSIDs with Wi-Fi network interfaces:

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
[a] monitoring transmissions among said plurality of stations to detect service set IDs associated therewith; and	The Huawei '678 Patent Accused Products comprise a policing station that can monitor transmissions among the plurality of stations to detect service set IDs associated therewith. For example, the monitor AP collects neighbor information including SSIDs:  As shown in the preceding figure, employees deploy unauthorized APs (rogue APs 1 and 2, which are Fat APs or smart terminals with the AP function enabled) to the WLAN of a company. Rogue AP 1 uses the SSID **Jack** and provides wireless services for an employee's own STA (such as a tablet). The company's WLAN may be interfered,

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	causing leakage of the company's information assets. Rogue AP 2 uses the same SSID as the WLAN system of the company, and attempts to steal company information assets by forging an authorized AP and establishing connections with devices in the company. In this case, the WIDS and WIPS functions can be enabled on the company's WLAN to contain rogue APs using the same SSID. After the WIDS and WIPS functions are configured on the AC, the monitor AP collects information about neighboring device and reports the information to the AC. When the AC identifies a rogue AP, it notifies the monitor AP of the rogue AP's identity information. The monitor AP then uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs associating with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This containment mechanism prevents STAs from associating with the rogue AP. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 22-23 (emphasis added).

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION

Table 2-3 Key information about a detected wireless device

Attribute	Description
MAC address	MAC address of the device
BSSID	BSSID of the device
Type	Ad hoc device, AP, STA, or wireless bridge
SSID	SSID of an ESS
Vendor	Vendor of the device
Channel	Channel in which the device is detected for the last time
RSSI	Maximum RSSI of the device
Beacon Interval	Interval at which an AP or ad hoc device sends Beacon frames
First Detected Time	First time at which the device is detected
Last Detected Time	Last time when the device is detected

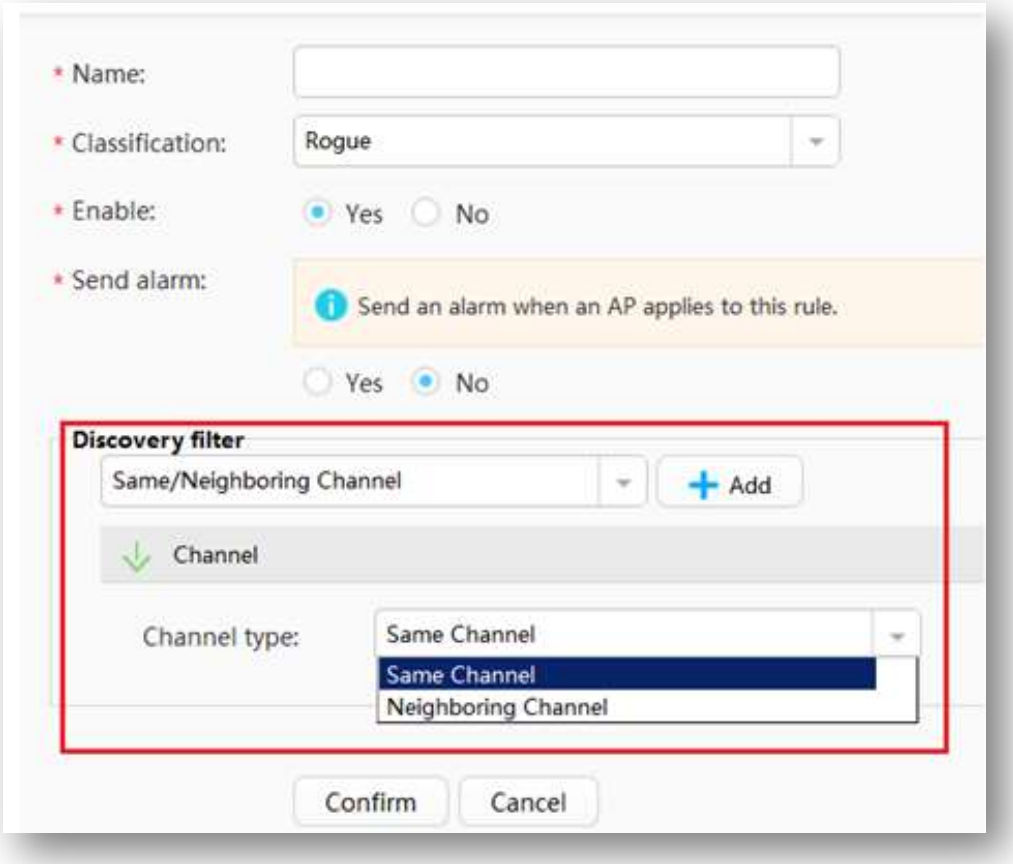
Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 9.

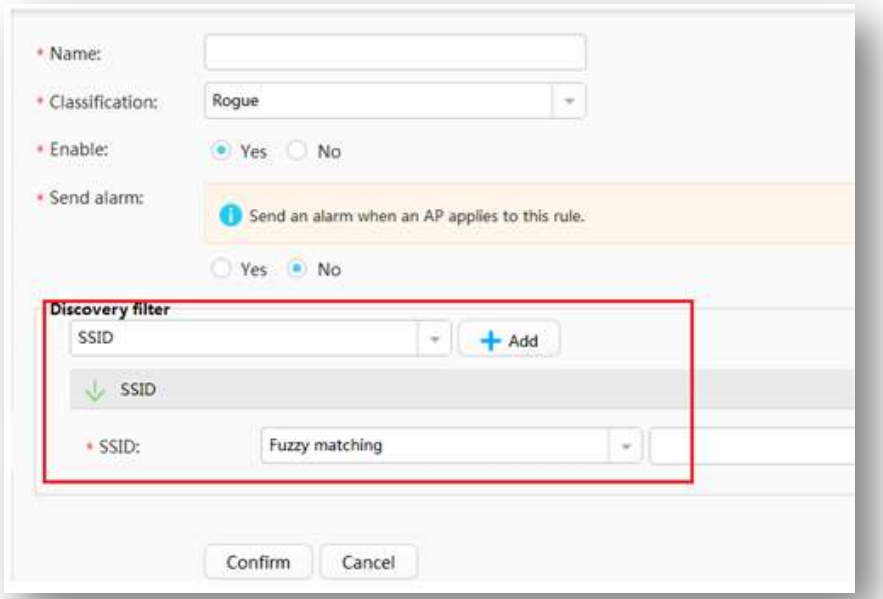
Further, the WIDS system, including as used in eSight, monitors transmissions among said plurality of stations to detect service set IDs associated therewith:

WIDS Wireless Intrusion Detection System

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security. … Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. Same or adjacent channel This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 SSID

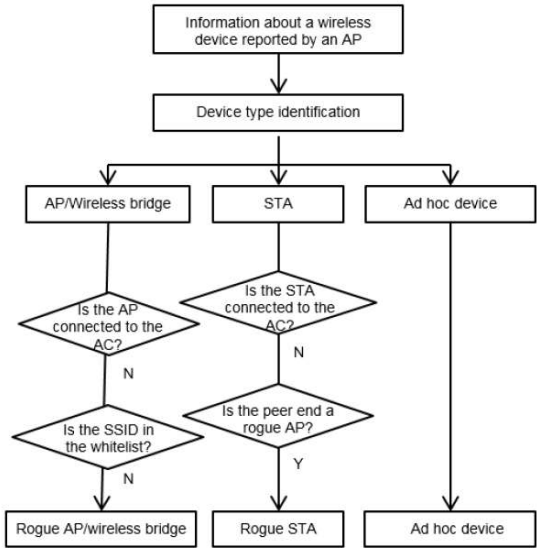
'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 The service set identifiers of networks from unauthorized vendors or wireless networks established by individuals are similar to authorized SSIDs. For example, the SSIDs are the same or characters are similar (such as 0 and o). In this case, users may be deceived to log in to rogue wireless networks. An SSID rule can be used to detect rogue APs whose SSIDs are similar to the authorized SSIDs or when a specified rule (regular expression) is met. HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for service set IDs, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also monitor for service set IDs. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.")
[b] generating an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network.	The Huawei '678 Patent Accused Products generate an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network. For example, when an AP's SSID is different than the SSID of the WLAN, it may be considered a Rogue AP and a Rogue AP alarm is generated.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION

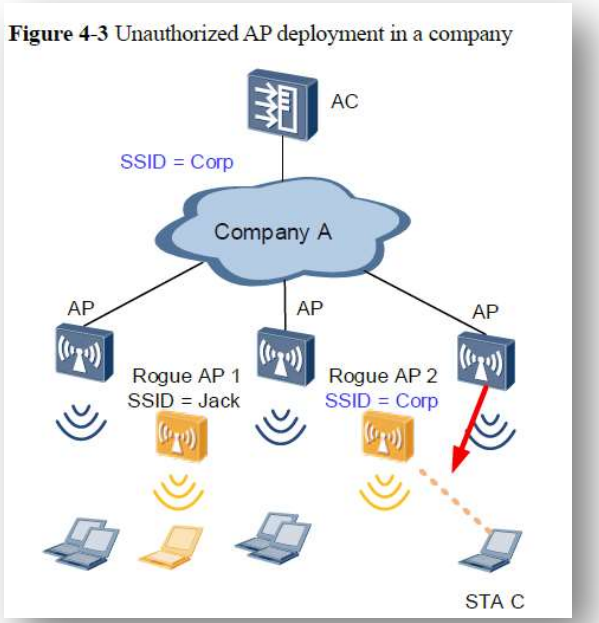
When receiving information about neighboring devices reported by an AP, an AC starts rogue device identification. The following figure shows the rogue device identification process.

Figure 2-7 Rogue device identification process



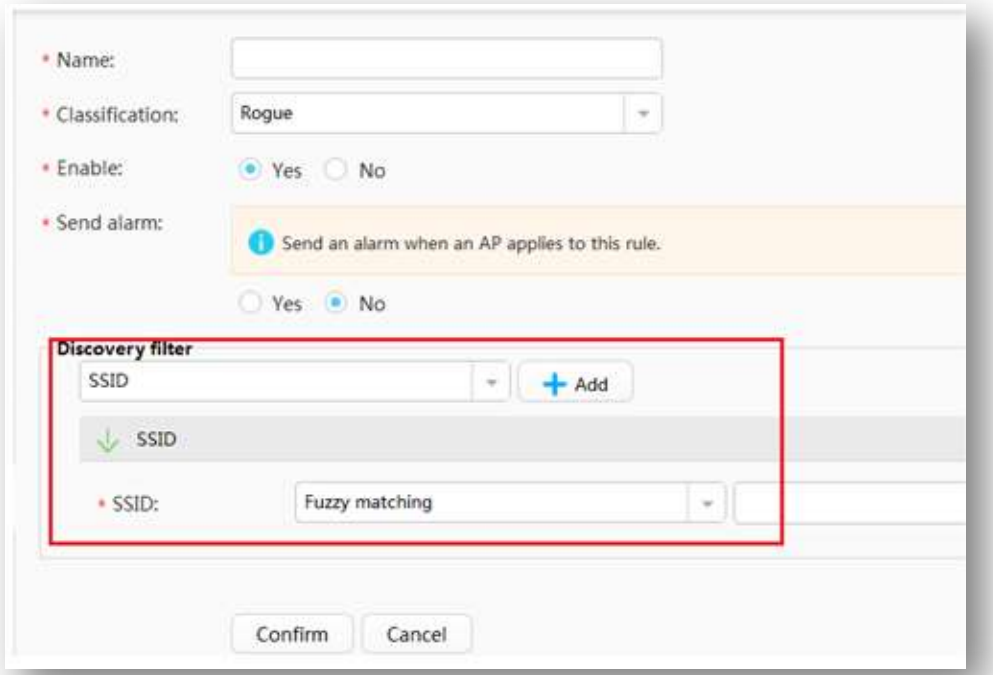
Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 9.

> To ensure data security or prevent interference to a WLAN, a company generally forbids deployment of unauthorized APs. In this case, the company can enable the WIDS function to detect other WLAN devices that do not belong to its own WLAN.

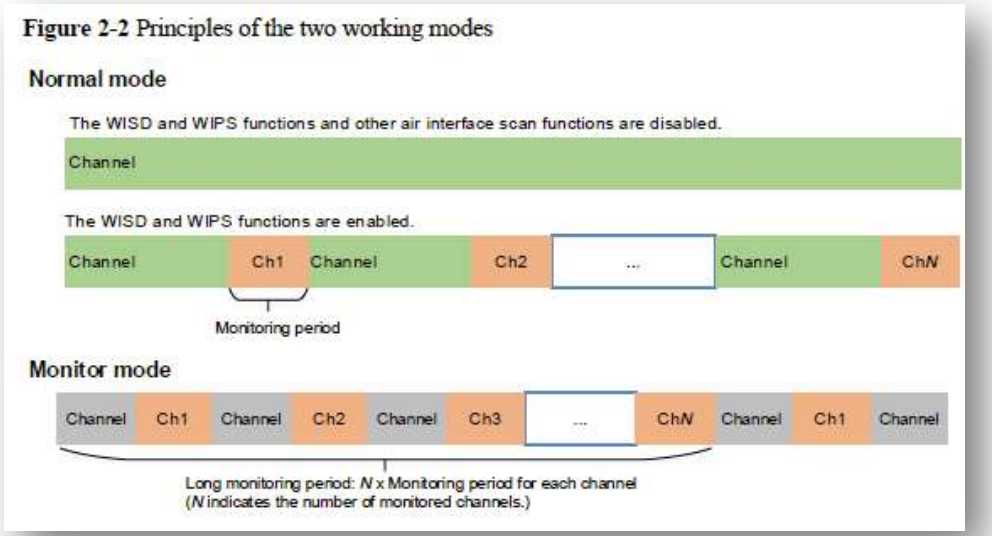
'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 As shown in the preceding figure, employees deploy unauthorized APs (rogue APs 1 and 2, which are Fat APs or smart terminals with the AP function enabled) to the WLAN of a company. Rogue AP 1 uses the SSID Jack and provides wireless services for an employee's own STA (such as a tablet). The company's WLAN may be interfered, causing leakage of the company's information assets. Rogue AP 2 uses the same SSID as the WLAN system of the company, and attempts to steal company information assets by forging an authorized AP and establishing connections with devices in the company.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	In this case, the WIDS and WIPS functions can be enabled on the company's WLAN to contain rogue APs using the same SSID. After the WIDS and WIPS functions are configured on the AC, the monitor AP collects information about neighboring device and reports the information to the AC. When the AC identifies a rogue AP, it notifies the monitor AP of the rogue AP's identity information. The monitor AP then uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs associating with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This containment mechanism prevents STAs from associating with the rogue AP. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 22-23. Rogue APs: Currently, Huawei WLAN devices support containment against …rogue APs with bogus SSIDs. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 11. If the device type is AP or wireless bridge, the AC first checks whether it is an authorized device. If the BSSID of the device is the same as that of another device currently managed by the AC, it is an authorized device. Otherwise, the identification continues. If the SSID of the device (such as CMCC) is in the SSID whitelist configured by the administrator, it is an authorized device. Otherwise, the device is identified as a rogue device. …. When the AC identifies an AP as a rogue AP, a rogue AP alarm is triggered and sent to the network management system (NMS) in an SNMP trap.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei Technologies Co., Ltd. WLAN WIDS & WIPS Technology White Paper; Issue 2.0 (2017-07-05) at 10. Further, the eSight White Paper describes using WIDS and generating an alarm based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network: SSID The service set identifiers of networks from unauthorized vendors or wireless networks established by individuals are similar to authorized SSIDs. For example, the SSIDs are the same or characters are similar (such as 0 and o). In this case, users may be deceived to log in to rogue wireless networks. An SSID rule can be used to detect rogue APs whose SSIDs are similar to the authorized SSIDs or when a specified rule (regular expression) is met.

'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	 HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12. *See also*: 3.1.25 WIDS Spoof SSID Profile WLAN services are available in public places, such as banks and airports. Users can connect to the WLANs after associating with corresponding SSIDs. If a rogue AP is

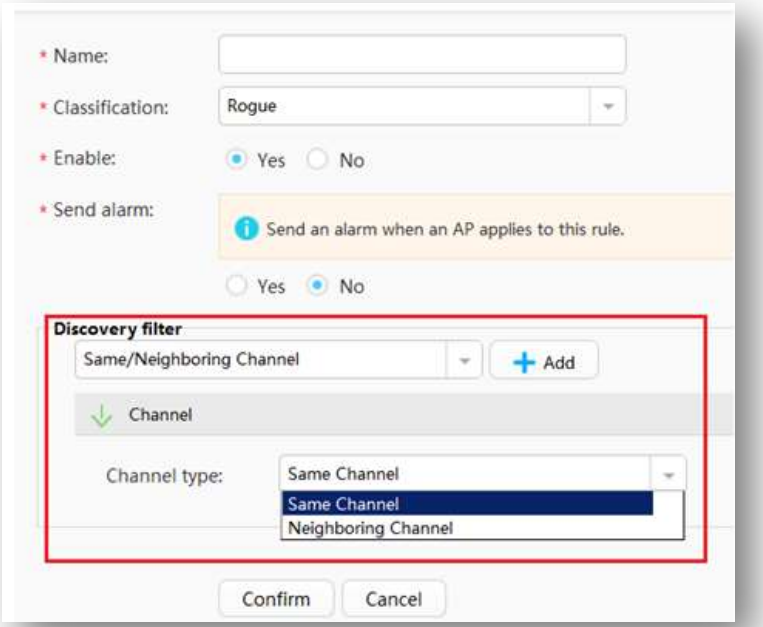
'678 PATENT CLAIM 17	INFRINGEMENT BY HUAWEI CORPORATION
	deployed and provides spoofing SSIDs similar to authorized SSIDs, the users may be misled and connect to the rogue AP, which brings security risks. To address this problem, configure a fuzzy matching rule to identify spoofing SSIDs. The device compares a detected SSID with the matching rule. If the SSID matches the rule, the SSID is considered a spoofing SSID. The AP using the spoofing SSID is a rogue AP. After rogue AP containment is configured, the device contains the rogue AP and disconnects users from the spoofing SSID. For the detailed configuration, see (Optional) Configuring Fuzzy Matching Rules for Identifying Spoofing SSIDs in the Configuration-WLAN Security Configuration Guide. HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 33. On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on monitoring for different service set IDs, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also generate an intrusion alert based on monitoring for different service set IDs. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'678 PATENT CLAIM 18	**INFRINGEMENT BY HUAWEI CORPORATION**
18. The wireless network of claim 12 wherein said plurality of stations transmit data over at least one channel; and wherein said policing station further detects transmissions over the at least one channel not originating from one of the plurality of stations and generates an intrusion alert based thereon.	The Huawei '678 Patent Accused Products infringe this claim. *See* Claim 12. Further, said plurality of stations transmit data over at least one channel; and wherein said policing station further detects transmissions over the at least one channel not originating from one of the plurality of stations (e.g., neighboring devices) and generates an intrusion alert based thereon. For example:  Rogue devices are detected in all the channels of the frequency band on which the current radio works, or channels allowed by a specified country code.

'678 PATENT CLAIM 18	INFRINGEMENT BY HUAWEI CORPORATION
	2.2.2 Wireless Device Identification On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows: 1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios. 2. The AC delivers the configuration to the AP. 3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames: − Beacon − Association Request − Association Response − Reassociation Request − Reassociation Response − Probe Response − Data frame 4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4.

'678 PATENT CLAIM 18	INFRINGEMENT BY HUAWEI CORPORATION
	Further, monitor APs monitor neighboring channels and detect transmissions of neighboring wireless devices. If these devices are determined to be Rogue APs, an intrusion alert is generated. ● Rogue AP: an unauthorized or malicious AP, which can be an AP that is connected to a network without permission, an unconfigured AP, a neighbor AP, or an AP manipulated by an attacker … ● Monitor AP: an AP that scans or listens on wireless channels and attempts to detect attacks to the wireless network. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 2; *see also* WLAN WIDS Technology White Paper, Issue 1.0 (2014-04-24) at 3. 2.2 Rogue Device Detection Rogue device detection of WLANs is enabled to monitor the entire network. Monitor APs are deployed on a WLAN that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless signals to detect rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3. After the WIDS and WIPS functions are configured on the AC, the monitor AP collects information about neighboring device and reports the information to the AC. When the AC identifies a rogue AP, it notifies the monitor AP of the rogue AP's identity information. Huawei Technologies Co., Ltd. WLAN WIDS & WIPS Technology White Paper; Issue 2.0 (2017-07-05) at 23.

'678 PATENT CLAIM 18	INFRINGEMENT BY HUAWEI CORPORATION
	When the AC identifies an AP as a rogue AP, a rogue AP alarm is triggered and sent to the network management system (NMS) in an SNMP trap. Huawei Technologies Co., Ltd. WLAN WIDS & WIPS Technology White Paper; Issue 2.0 (2017-07-05) at 10. As further described in the eSight documentation: 3.2.3 WIDS Wireless Intrusion Detection System The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security. . . . Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. ● Same or adjacent channel

'678 PATENT CLAIM 18	INFRINGEMENT BY HUAWEI CORPORATION
	This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference  HUAWEI eSight WLAN Technology White Paper, Issue 1.0 (2017-03-20) at 10-12. On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on detecting transmissions over the at least one channel not originating from one of the plurality of stations, including when configured as a mobile hotspot.

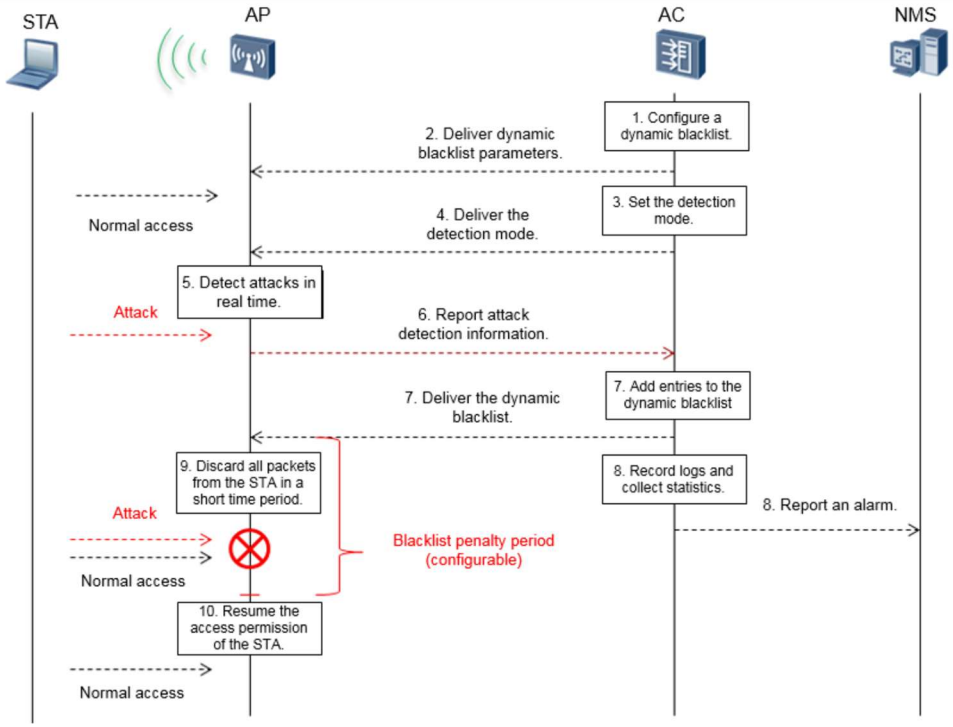
'678 PATENT CLAIM 18	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also generate an intrusion alert based on detecting transmissions over the at least one channel not originating from one of the plurality of stations. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'678 PATENT CLAIM 19	INFRINGEMENT BY HUAWEI CORPORATION
19. The wireless network of claim 12 wherein said policing station further transmits an intrusion alert to at least one of said plurality of stations.	The Huawei '678 Patent Accused Products infringe this claim. *See* Claim 12. Further, said policing station further transmits an intrusion alert to at least one of said plurality of stations. For example, the monitor AP generates and transmits intrusion alert information to the AC, and the AC reports intrusion alert information to other APs: On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows:

'678 PATENT CLAIM 19	INFRINGEMENT BY HUAWEI CORPORATION
	1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios. 2. The AC delivers the configuration to the AP. 3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames: – Beacon – Association Request – Association Response – Reassociation Request – Reassociation Response – Probe Response – Data frame 4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4.

***Harris Corporation v. Huawei, et al* - Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
~~CORRECTED~~ AMENDED Exhibit E – U.S. Patent No. 7,224,678 ('678) – Claims 12-13, 17-20, 51-52, 56-58

'678 PATENT CLAIM 19	INFRINGEMENT BY HUAWEI CORPORATION



…

5. The AP detects attacks in attack detection mode delivered by the AC.

6. When the AP detects an attack, it reports attack information to the AC, such as the MAC address of the attacking device and the attack type. After receiving the attack information, the AC adds the attacking device to the attacking device list. If the AP

'678 PATENT CLAIM 19	INFRINGEMENT BY HUAWEI CORPORATION
	detects no attack from this attacking device in the next three attack detection periods, it requests the AC to delete the attacking device from the list. 7. The AC determines whether to add the attacking device to the dynamic blacklist. It records detected brute force PSK crackers to the dynamic blacklist cache table, and delivers the table to the AP. 8. The AC collects statistics on attack types and sends trap messages to report the attack types to the NMS. 9. After receiving the dynamic blacklist, the AP discards the packets from the attacking devices in the dynamic blacklist. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 17 (emphasis added). If so, the AP considers that the STA is using the brute force method to crack the password and reports an alarm to the AC. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 15. □ The AP listens on frames to collect information about neighboring wireless devices, and reports the information to the AC at the specified short interval. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC.

'678 PATENT CLAIM 19	INFRINGEMENT BY HUAWEI CORPORATION
	The AP reports full information about all detected wireless devices to the AC at the long interval for information synchronization. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 8. On information and belief Huawei consumer devices, including laptops, phones and tablets also can transmit intrusion alerts, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also transmit intrusion alerts. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'678 PATENT CLAIM 20	INFRINGEMENT BY HUAWEI CORPORATION
20. The wireless network of claim 12 wherein said policing	The Huawei '678 Patent Accused Products infringe this claim. *See* Claim 12.

'678 PATENT CLAIM 20	**INFRINGEMENT BY HUAWEI CORPORATION**
station comprises a base station.	Further the policing station comprises a base station. For example, the monitor APs described above acts as a base station. *See* Claim 12

'678 PATENT CLAIM 51	**INFRINGEMENT BY HUAWEI CORPORATION**
51. An intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations, the method comprising:	The Huawei '678 Patent Accused Products infringe this claim. Huawei makes, uses, sells, offers to sell and/or imports equipment used in wireless or metropolitan local area networks (WLAN products), and on information and belief, makes, uses, sells, offers to sell and/or imports such networks in the United States. Such equipment and networks perform an intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations. *See* evidence for Claim 12[preamble]. The method further comprises the steps below.
[a] transmitting data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith;	Huawei '678 Patent Accused Products transmit data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith. *See* evidence for Claim 12[a].

'678 PATENT CLAIM 51	**INFRINGEMENT BY HUAWEI CORPORATION**
[b] monitoring transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses; and	Huawei '678 Patent Accused Products monitor transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses. *See* evidence for Claim 12[c].
[c] generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.	Huawei '678 Patent Accused Products generate an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address. *See* evidence for Claim 12[d].

'678 PATENT CLAIM 52	**INFRINGEMENT BY HUAWEI CORPORATION**
52. The method of claim 51 wherein generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address comprises generating an intrusion alert based upon detecting the number of failed attempts to authenticate the MAC address within a predetermined period.	Huawei '678 Patent Accused Products infringe this claim. *See* Claim 51. Further, generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address comprises generating an intrusion alert based upon detecting the number of failed attempts to authenticate the MAC address within a predetermined period *See* evidence for Claim 13.

'678 PATENT CLAIM 56	**INFRINGEMENT BY HUAWEI CORPORATION**
56. The method of claim 51 wherein the wireless network has at least one service set identification (ID) associated therewith; and further comprising:	The Huawei '678 Patent Accused Products infringe this claim. *See* claim 51. Further, the wireless network has at least one service set identification (ID) associated therewith. *See* evidence for Claim 17[preamble].
[a] monitoring transmissions among the plurality of stations to detect service set IDs associated therewith; and	The Huawei '678 Patent Accused Products monitor transmissions among the plurality of stations to detect service set IDs associated therewith. *See* evidence for Claim 17[a].
[b] generating an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network.	The Huawei '678 Patent Accused Products generate an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network. *See* evidence for Claim 17[b].

'678 PATENT CLAIM 57	**INFRINGEMENT BY HUAWEI CORPORATION**
57. The method of claim 51 wherein transmitting data	The Huawei '678 Patent Accused Products infringe this claim. *See* claim 51. Further, transmitting data comprises transmitting data over at least one channel; and further comprising detecting transmissions over

'678 PATENT CLAIM 57	**INFRINGEMENT BY HUAWEI CORPORATION**
comprises transmitting data over at least one channel; and further comprising detecting transmissions over the at least one channel not originating from one of the plurality of stations and generating an intrusion alert based thereon.	the at least one channel not originating from one of the plurality of stations and generating an intrusion alert based thereon. *See* evidence for Claim 18.

'678 PATENT CLAIM 58	**INFRINGEMENT BY HUAWEI CORPORATION**
58. The method of claim 51 further comprising transmitting the intrusion alert to at least one of the plurality of stations.	The Huawei '678 Patent Accused Products infringe this claim. *See* Claim 51. The instrumentalities further transmit the intrusion alert to at least one of the plurality of stations. *See* evidence for Claim 19.